Benutzerhandbuch

WinRoute Pro 4.1

Tiny Software Inc.

Inhalt

Installation und Konfiguration Kapitel 2

Einsatzbeispiele Kapitel 3

Firewall-Konfiguration Kapitel 4

EINLEITUNG

Sehr geehrter Kunde,

danke, dass Sie WinRoute Pro erworben haben bzw. testen. Tiny Software ist ein in der Firewall-Technologie für kleine und mittelgroße Netzwerke führendes Unternehmen und hat sehr viel Arbeit in die Forschung investiert, um Ihnen einen leistungsstarken und dennoch einfachen Router bzw. eine Firewall für Windows-Betriebssysteme anbieten zu können.

WinRoute Pro ist eine Netzwerkanwendung, die in Verbindung mit einem PC teurere, auf reiner Hardware basierende Router und Firewalls ausgezeichnet ersetzt. Um die Anwendung nutzen zu können, muss das Netzwerk ordnungsgemäß eingerichtet und konfiguriert sein. Daher sind einige Erfahrungen mit Netzwerkumgebungen notwendig.

Wir weisen darauf hin, dass (nach unserer Statistik) 90 % der Probleme, die Kunden beim Verbinden ihres Netzwerks mit dem Internet haben, auf eine unsachgemäße Netzwerkkonfiguration zurückzuführen sind. Dieses Handbuch enthält einige Beispiele für die Netzwerkkonfiguration. Die Installation kann jedoch auf Grund verschiedener Besonderheiten davon abweichen.

Wir empfehlen Ihnen dringend, diese Dokumentation sehr aufmerksam und genau durchzulesen. Sie wurde für Benutzer erstellt, die bereits über grundlegende Netzwerkkenntnisse verfügen sowie die Fähigkeit und das Know-how besitzen, ein lokales Netzwerk (Local Area Network = LAN) zu installieren.

Falls Sie weitere Tipps, Checklisten und aktualisierte Versionen benötigen, ziehen Sie zunächst die Online-Hilfe zu Rate, bevor Sie den technischen Support anrufen.

Wir danken Ihnen nochmals dafür, dass Sie WinRoute erworben haben bzw. testen.

Mit freundlichen Grüßen

TINY SOFTWARE, INC.

KAPITEL 1

WINROUTE-BESCHREIBUNG

In diesem Kapitel

WinRoute-Zusammenfassung

WinRoute Pro ist die neueste **Internet Router- und Firewall-**Software, mit der alle Computer Ihres Netzwerkes praktisch mühelos so eingerichtet werden können, dass sie eine einzelne Internetverbindung gemeinsam nutzen können! Stellen Sie die Verbindung über DFÜ, DSL, Kabel, ISDN, LAN, T1, Radio, DirecPC her. So einfach ist das!

Fernverwaltung

WinRoute Administrator stellt die Konfiguration und Einstellungen auf der WinRoute Engine bereit. Bei WinRoute Administrator handelt es sich um eine separate Anwendung (wradmin.exe), die von jedem Computer im Netzwerk ausgeführt werden kann, mit dem der WinRoute Engine-Computer verbunden ist. Der Zugang zur Engine ist durch eine komplizierte Verschlüsselung und ein Kennwort gesichert.

Protokollierung

WinRoute Pro verleiht jedem Administrator völlige Kontrolle über den Datenverkehr, der durch den Host-Computer, auf dem das Programm ausgeführt wird, fließt. Der Administrator profitiert von der Analyse des Datenflusses von TCP, UDP, ICMP, ARP-Paketen, DNS-Abfragen, Treiberinformationen und vielem mehr. Jeder Vorgang ist mit einem Zeitstempel versehen.

NAT-Router

WinRoute umfasst die beste heute verfügbare Implementierung der Network Address Translation-Technik (= Übersetzen und Verstecken der lokalen IP-Adressen hinter einer einzigen ausgehenden IP-Adresse). Es ist darauf ausgelegt, den Benutzern die neueste Routing-Funktion und den neuesten Netzwerkschutz zur Verfügung zu stellen. Der NAT-Treiber, der für WinRoute exklusiv entwickelt wurde, bietet eine Sicherheitslösung, die mit teureren Produkten vergleichbar ist, dabei aber wesentlich weniger kostet.

Erweitertes NAT-Routing

Mit erweitertem NAT-Routing hat der Benutzer die Option, die IP-Quelladresse ausgehender Pakete nach verschiedenen Kriterien zu ändern. Damit ist eine einfache Integration lokaler Netzwerke (LANs) mit WinRoute in die WAN-Umgebung des Unternehmens mit verschiedenen Segmenten, entmilitarisierten Zonen, virtuellen privaten Netzwerken usw. gewährleistet.

Hosting-Server hinter WinRoute

WinRoute schließt standardmäßig alle Anschlüsse, um maximale Sicherheit zu gewähren. Daher werden alle nicht eingeleiteten Anforderungen abgewiesen, es sei denn eine Zuordnung wurde erstellt. Mit Hilfe der Anschlusszuordnung kann der Benutzer entscheiden, wie er IP-Pakete, die über eine beliebige WinRoute-Schnittstelle transportiert werden, umleiten möchte. Mit WinRoute können Benutzer Pakete, die über einen bestimmten Anschluss eingehen, an einen festgelegten internen Computer weitergegeben. So kann ein Web-Server, MAIL-Server, FTP-Server, VPN-Server oder praktisch jeder andere Servertyp sicher hinter der Firewall verwendet werden.

Firewall-Sicherheit

Durch die Kombination aus NAT-Architektur und der Fähigkeit, auf niedriger Ebene zu arbeiten, bietet WinRoute Benutzern eine Firewall-Funktion, die mit teureren Lösungen vergleichbar ist. Dadurch kann WinRoute sowohl eingehende als auch abgehende Pakete erfassen, wodurch es gegenüber Angriffen geschützt ist. Anti-Spoofing ist eine Ergänzung zur Paketfilterung von WinRoute. Es schützt das LAN gegen Angriffe durch unberechtigte Benutzer mit gefälschten IP-Quelladressen schützt.

Einfache Netzwerkkonfiguration

Der DHCP-Server und die DNS-Weiterleitung, die in WinRoute Pro enthalten sind, vereinfachen die Verwaltung der Netzwerkkonfiguration. Beide Komponenten stellen ausgereifte Techniken dar. Der DHCP-Server von WinRoute kann problemlos den in Windows NT enthaltenen DHCP-Server ersetzen.

MAIL-Server

Der MAIL-Server von WinRoute ist äußerst vielseitig. Er ist mit SMTP/POP3 kompatibel, verfügt über nahezu unbegrenzte Aliaszuordnungsmöglichkeiten und bietet eine automatische E-Mail-Sortierung. Die Benutzer können eine oder mehrere E-Mail-Adressen verwenden und effizient in Gruppen arbeiten (d. h. Vertrieb, Support usw.). Alle diese Funktionen sind ungeachtet der verwendeten Internetverbindung verfügbar.

HTTP-Cache

Die Architektur von WinRoute beinhaltet eine innovative Cache-Engine. Im Gegensatz zu PROXY-Servern mit Cache-Funktionen speichert der Cache von WinRoute die übertragenen Daten in einer einzigen Datei mit vordefinierter Länge, anstatt für jedes Objekt eine separate Datei zu verwenden. So wird vom Cache belegter Festplattenspeicher eingespart, und zwar insbesondere in FAT16-Umgebungen (hauptsächlich Windows 95).

Umfangreiche Protokollunterstützung

WinRoute unterstützt alle Internet-Standardprotokolle:

IPSEC, H.323, NetMeeting, Net2Phone, WebPhone, UnixTalk, RealAudio, RealVideo, ICA Winframe, IRC, FTP, HTTP, Telnet, PPTP, Traceroute, Ping, Year 2000, Aol, chargen, cuseeme, daytime, discard, dns, echo, finger, gopher, https, imap3, imap4, ipr, IPX overIP, netstat, nntp, ntp, ping, pop3, radius, wais, rcp, rlogin, rsh, smtp, snmp, ssl, ssh, systat, tacacs, uucpover IP, whois, xtacacs.

NAT-Router

In diesem Abschnitt

Einführung in NAT

NAT - Network Address Translation

Network Address Translation (NAT) gehört zu den leistungsstärksten Sicherheitsfunktionen von WinRoute. NAT ist ein Internet-Standardprotokoll, mit dem sich private Netzwerkadressen hinter einer einzelnen Adresse oder mehreren Adressen "verstecken" lassen. "IP Masquerading", eine Version von NAT, wird bereits seit vielen Jahren von Linux-Anwendern verwendet. WinRoute ist eines der wenigen Produkte für die Windows-Plattform, das NAT-Funktionen auf Einstiegsebene bietet.

NAT kann auf verschiedene Arten implementiert werden. Im Wesentlichen schafft es jedoch einen nahezu unbegrenzten privaten Adressbereich für interne Netzwerke, der von WinRoute "übersetzt" wird. Auf diese Weise können Daten zu und von öffentlichen Netzwerken übertragen werden, ohne dass Informationen über sensible interne Netzwerke preisgegeben werden. Ist der private Adressbereich an der internen Schnittstelle einer WinRoute-Firewall nicht bekannt, so ist es praktisch unmöglich, ein System im internen Netzwerk, das NAT verwendet, direkt anzugreifen.

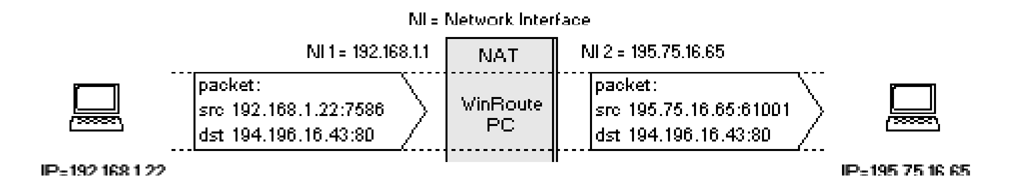
So funktioniert NAT

Network Address Translation (NAT) ist ein Prozess, mit dem Pakete, die von und zu einem lokalen Netzwerk (LAN), von oder zum Internet oder einem anderen auf IP-basierenden Netzwerk gesendet werden, modifiziert.

Ausgehende Pakete

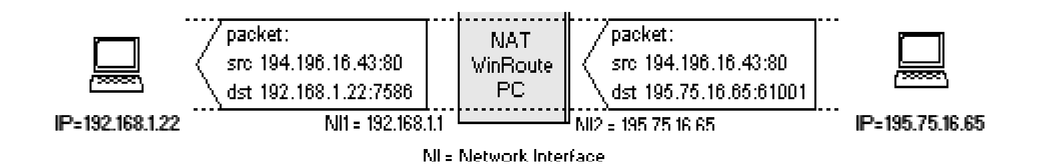
Pakete, die auf dem Weg **vom** LAN die Network Address Tranlation Engine passieren, werden so verändert oder übersetzt, dass sie aussehen, als kämen sie von dem NAT ausführenden Computer. (Dieser Computer ist direkt mit dem Internet verbunden.) Im Grunde wird jedoch nur die IP-"Quelladresse" im Header durch die öffentliche IP-Adresse des "NAT"-Computers ersetzt.

Die NAT-Engine erstellt darüber hinaus eine Datensatztabelle für jedes Paket, das das Internet passiert hat.



Eingehende Pakete
Pakete, die NAT auf dem Weg **zum** LAN passieren, werden mit den von der NAT-Engine gespeicherten Datensätzen verglichen. Dabei wird die IP-"Zieladresse" basierend auf Datensätzen in der Datenbank wieder auf die spezifische interne private IP-Adresse zurückgeändert, um den Computer im LAN zu erreichen.

Das Paket kommt am NAT-Computer mit der öffentlichen IP-Adresse des NAT-Computers als Zieladresse an. Die NAT-Engine ändert diese Information dann, um das Paket dem richtigen Empfänger innerhalb des lokalen Netzwerks zuzustellen.



Aufbau von WinRoute

WinRoute-Architektur

Für erweitertes Internetworking ist es hilfreich, die Funktionsweise von WinRoute zu verstehen. Die unten aufgeführten Erläuterungen und Beispiele zeigen, dass WinRoute eine ausgezeichnete Lösung für nahezu jede Netzwerkkonfiguration darstellt.

1. **Vollständige Sicherheit**
   WinRoute arbeitet **unterhalb des TCP-Stack** auf der IPSEC-Ebene. Mit anderen Worten, es fängt **ausgehende** und **eingehende** Pakete ab, **BEVOR** sie auf Ihren Computer gelangen können.

Durch dieses fortschrittliche Konzept ist die Sicherheit von WinRoute beinahe **unantastbar.**

WinRoute (Proxy,Mail, DNS, DHCP server)				
windows sockets				
TCP/IP protocol				
WinRoute inpection module (anti-spoofing, packet filter, NAT)				
network adapter driver		WAN subsystem		…
network adapter		modem	ISDN	…

2. **Vollständige Protokollunterstützung**
   WinRoute ist ein Software-ROUTER. Als solcher kann es im Gegensatz zu Proxy-Servern wie WinGate oder WinProxy beinahe jedes Internet-Protokoll passieren lassen. Gleichzeitig überprüft WinRoute jedes Paket anhand der in der Software integrierten erweiterten Sicherheits- und Firewall-Funktionen. Bei Systemen, auf denen Windows 95 und 98 ausgeführt wird, organisiert WinRoute die Weiterleitung der Pakete. Bei Systemen mit Windows NT, führt das NT-Betriebssystem die Weiterleitung aus, und WinRoute verwaltet den NAT-Dienst sowie andere Daten.

3. **Vollständige Flexibilität**
   WinRoute führt NAT (Network Address Translation) an den Schnittstellen Ihrer Wahl durch. Außerdem führt es an den entsprechenden Schnittstellen alle voreingestellten Sicherheitsroutinen durch. Dadurch hat der Benutzer bei der Gestaltung und Konfiguration der Sicherheitsoptionen viel Freiraum.

NAT an beiden Schnittstellen einstellen

Unter Umständen möchten Sie WinRoute nur als **neutralen Zugangs-Router** für den Datenverkehr (Pakete) verwenden, der vom **Internet** zu einem **lokalen Netzwerk** fließt. Wenn Sie bereits einen gemeinsamen Internetzugang besitzen, jedoch keine vom Internet zugänglichen Server und Anwendungen in Ihrem privaten Netzwerk ausführen können, dann ist WinRoute in dieser speziellen Konfiguration möglicherweise genau die richtige Lösung.

Folgende Dienste sollten vom Internet aus zugänglich sein:

- Telnet-Server (z. B. AS400)
- WWW-Server
- Mail-Server
- PC Anywhere
- FTP-Server
- … und jeder andere Server (Dienst), der an einem bestimmten Anschluss zugänglich ist.

WinRoute bietet den Benutzern bzw. Kunden zuverlässigen und sicheren Zugang zu diesen Diensten. Die Konfiguration von WinRoute für diese Dienste wird in anderen Kapiteln beschrieben. Folgende Einstellungen werden auf andere Weise vorgenommen:

Funktion	Ursprünglich empfohlen	In diesem Fall
NAT an der Internet-Schnittstelle	EIN	EIN
NAT an der internen (LAN-) Schnittstelle	AUS	EIN
Die IP-Adresse der internen Schnittstelle von WinRoute als Standard-Gateway für die anderen Computer innerhalb des Netzwerks	JA (obligatorisch)	NEIN (optional)

Mit anderen Worten heißt das, mit WinRoute können Sie bestimmte Dienste vom Internet aus zugänglich machen, OHNE die Netzwerkkonfiguration ändern zu müssen.

Hinweis! Wenn Sie NAT an beiden Schnittstellen einrichten, können Sie WinRoute NICHT für den gemeinsamen Internetzugang verwenden!

Die Einstellungen für den Standard-Gateway in diesem Beispiel verleihen Ihnen viel Freiraum. Alle vorhandenen Umgebungen können Sie unverändert lassen. Um alle bereits in Ihrem Netzwerk eingerichteten Router und Routen funktionsfähig zu halten, können Sie durch Hinzufügen neuer Computer, die WinRoute ausführen, externen Benutzern Zugang zu den Servern Ihres lokalen Netzwerks gewähren.

Dies ist ideal, wenn Sie beispielsweise über ein bestehendes WAN (Wide Area Network) verfügen und einem externen Benutzer Zugang zu Ihrer AS400 (Telnet-Server) oder Ihrem internen Netzwerk mittels PPTP gewähren möchten.

Führen Sie dazu folgende Schritte aus:

1 Schließen Sie einen Computer mit zwei Schnittstellen an Ihr Netzwerk an. Eine (externe) Schnittstelle stellt die Verbindung zum Internet her, eine andere (interne) Schnittstelle die Verbindung zum vorhandenen Netzwerk.

2 Weisen Sie der externen Schnittstelle eine IP-Adresse zu, mit der auf die Dienste/Server zugegriffen wird, die Sie vom Internet aus zugänglich machen möchten.

3 Weisen Sie die interne IP-Adresse entweder manuell oder über den DHCP-Server zu.

4 Richten Sie WinRoute so ein, dass NAT an beiden Schnittstellen durchgeführt wird.

5 Richten Sie für die Dienste, die Sie innerhalb Ihres Netzwerks ausführen möchten, die Anschlusszuordnung ein.

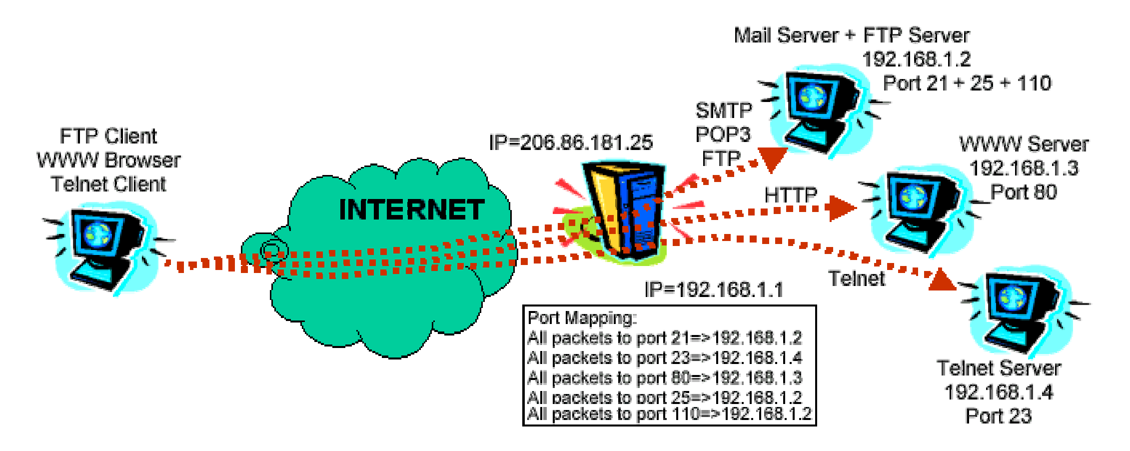
Nach Vornehmen dieser Einstellungen erhalten externe Benutzer vom Internet aus Zugang zu Ihren internen Diensten, die an bestimmten Anschlüssen ausgeführt werden. Für die Sicherheit eines solchen Zugangs sorgt die Firewall von WinRoute.

Anschlusszuordnung - Paketweiterleitung

WinRoute führt NAT durch und macht somit das geschützte Netzwerk von außen unzugänglich. Durch die Anschlusszuordnung (oder Port Address Translation - PAT) werden öffentliche Dienste, wie beispielsweise ein Internetserver oder ein FTP-Server sowie andere auf Ihrem privaten Netzwerk laufende Server vom Internet aus zugänglich.

So funktioniert die Anschlusszuordnung

Jedes Paket, das von außerhalb des Netzwerkes (aus dem Internet) eingeht, wird daraufhin überprüft, ob seine Eigenschaften (d. h. das Protokoll, der Zielanschluss und die IP-Zieladresse) mit dem jeweiligen Eintrag in der Anschlusszuordnungstabelle übereinstimmen (Protokoll, Zielanschluss, IP-Zieladresse). Wenn das eingehende Paket die gewünschten Kriterien erfüllt, wird das Paket modifiziert und an die IP-Adresse, die im geschützten Netzwerk als "Ziel-IP" im Tabelleneintrag definiert wird, und an den als "Zielanschluss" definierten Anschluss gesendet.



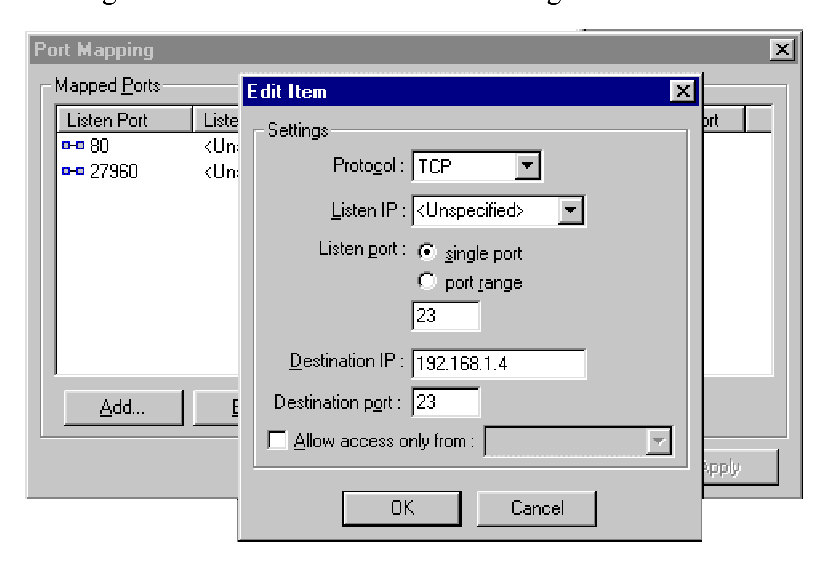
Wenn Sie beispielsweise einen Web-Server der internen IP 192.168.1.3 verwenden und Benutzern aus dem Internet Zugang zu diesem gewähren möchten, wird es Anfragen von Internet-Benutzern an ihren WinRoute-Computer geben. Diese besitzen externe IP-Adressen, die dem DNS-Eintrag (Domain Name Server) Ihres Web-Servers www.ihredomäne.com gleichen. Da alle Anfragen an den Web-Server am Anschluss 80 eingehen, sollten Sie die Anschlusszuordnung so einstellen, dass die gesamte TCP-Kommunikation am Anschluss 80 zur IP-Adresse 192.168.1.3 umgeleitet wird.

Die Konfiguration der Anschlusszuordnung

So richten Sie die Anschlusszuordnung ein:

1 Gehen Sie in das Menü *Einstellungen->Erweitert->Anschlusszuordnung.*

2 Fügen Sie eine neue Anschlusszuordnung hinzu.



Protokoll

Wählen Sie das Protokoll aus, das von Anwendung/Dienst benutzt wird. Einige Anwendungen/Dienste verwenden das TCP- und UDP-Protokoll zusammen. Beispielsweise WinRoute-Aministrator-Modul.

Überwachungs-IP

Die IP-Adresse, an die die eingehenden Pakete gesendet werden. Normalerweise ist dies die IP-Adresse, die mit Ihrer Internet-Schnittstelle assoziiert ist. Hinweis: Es kann sein, dass mehrere IP-Adressen mit einer Schnittstelle assoziiert werden.

Überwachungsanschluss

Die Nummer des Anschlusses, an dem die Pakete eingehen.

Ziel-IP

Die IP-Adresse innerhalb Ihres lokalen Netzwerks, die Ihren Server (Dienst) betreibt, der eingehende Pakete (Web-Server, FTP-Server etc.) beantwortet.

Zielanschluss

Der Anschluss, an dem die Anwendung überwacht wird. Üblicherweise die gleiche Nummer wie die Überwachungsanschlüsse.

Zugang nur gewähren von

Sie können die Adresse spezifizieren, von der aus Sie den Zugang ermöglichen möchten. Dies ist für die Erhöhung der Sicherheit sehr wichtig, falls Sie die Anschlusszuordnung für Fernverwaltungsanwendungen wie den WinRoute-Administrator, PC Anywhere etc. einrichten. Sie können die Gruppe der IP-Adressen festlegen. Zunächst müssen Sie eine solche Gruppe im Dialogfeld "Adressengruppe" erstellen.

Anschlusszuordnung für Systeme mit mehreren IP-Adressen

Sie können Ihrer Internet-Schnittstelle mehrere IP-Adressen zuweisen und mehrere Dienste, die Sie vom Internet aus zugänglich machen möchten, innerhalb Ihres Netzwerks bereitstellen.

5 x WWW-Server

Angenommen, Sie möchten mit 5 Web-Servern arbeiten, wovon jeder eine separate Domäne besitzt, die mit einer anderen IP-Adresse assoziiert ist.

In einem solchen Fall richten Sie 5 IP-Adressen an Ihrer externen Schnittstelle (welche die Verbindung mit dem Internet herstellt) ein und arbeiten mit Web-Servern auf anderen Computern in Ihrem internen Netzwerk.

Jeder Web-Server kann auf einem separaten Computer ausgeführt werden, oder Sie können mehrere IP-Adressen einem Computer in Ihrem internen Netzwerk zuweisen und alle Web-Server über diesen Computer ausführen.

Anschließend richten Sie 5 Anschlusszuordnungen im Dialog Anschlusszuordnung fest. Für jeden Web-Server definieren Sie Folgendes:

- IP-Überwachungsadresse (die öffentliche IP-Adresse, die mit der Domäne assoziiert ist)
- Überwachungsanschluss: in unserem Fall 80
- IP-Zieladresse: die IP-Adresse, auf der der Web-Server arbeitet.
- Zielanschluss: 80 (für www)

Weitere Beispiele zur erweiterten Anschlusszuordnung finden Sie im Kapitel zum erweiterten (Inter-)Networking.

Mehrfach-NAT

WinRoute ermöglicht eine einfache NAT (Network Address Translation) und auch kompliziertere Einstellungen. Sie können anhand der IP-Quelladresse oder der IP-Zieladresse des Paketes festlegen, dass NAT mit einer anderen IP-Adresse ausgeführt wird (d. h. dass Pakete so aussehen würden, als stammten sie von einer anderen IP-Adresse) oder dass NAT überhaupt nicht ausgeführt wird.

Solche Einstellungen sind in anspruchsvolleren Netzwerken sehr wichtig, bei denen:

- bestimmte Computer eine andere IP-Adresse aufweisen sollen als die Hauptadresse, die vom Rest des Netzwerks genutzt wird.
- Sie Zweigniederlassungen mit dem WAN (Wide Area Network) mit privatem Adressplatz verbunden haben und sich alle einen Internetzugang teilen sollen.
- sich Mehrfachsegmente im Hintergrund von WinRoute befinden, von denen ein oder mehrere Segmente DMZ(s) mit öffentlichen IP-Adressen sind.
- Sie innerhalb Ihres privaten Netzwerks über öffentliche IP-Adressen verfügen möchten. (Denken Sie daran, mit Ihrem Internetdiensteanbieter abzusprechen, dass diese IP-Adressen an Ihre IP-Adresse geleitet werden.)

Beispiele für erweiterte NAT-Einstellungen finden Sie im Kapitel über zum erweiterten (Inter-)Networking.

IP-Quelladresse, IP-Zieladresse

Sie können erweiterte NAT-Einstellungen durchführen, die auf der IP-Adresse basieren, von der aus die Pakete gesendet werden (Quelle) oder an die sie gesendet werden (Ziel). Als Quelle können Sie die Host-IP eingeben, das gesamte Netzwerk (durch Netzwerk-Maske begrenzt) oder die Gruppe der IP-Adressen, die zuvor im Menü *Einstellungen->Erweitert->Adressengruppen* erstellt wurde.

Keine NAT durchführen

Falls ausgewählt, werden die in das Internet versandte Pakete nicht verändert.

NAT mit spezieller IP-Adresse durchführen

Falls ausgewählt, werden die in das Internet versandte Pakete so verändert, als stammten sie von der gewünschten IP-Adresse.

VPN-Unterstützung

Wie bereits erwähnt, ist WinRoute dem Datenstrom der beiden heute gängigsten VPN-Protokolle durchaus gewachsen: Dem IP Security-Protokoll (IPSec) von der IETF (Internet Engineering Task Force) sowie dem Point-to-Point-Tunneling-Protokoll, das in den letzten Jahren auf Grund der Integration in die Software des Client-Betriebssystems von Microsoft Windows bekannt wurde.

Schnittstellentabelle

Die Schnittstellentabelle ist ein Dialog, in dem WinRoute alle im Computer verfügbaren Schnittstellen, die es erkennen konnte, anzeigt. Wenn Sie mehr Schnittstellen haben sollten als WinRoute darstellt, ist es wahrscheinlich, dass Treiber für solche Schnittstellen vom Betriebssystem nicht richtig geladen wurden und WinRoute diese nicht erkennen konnte.

Es wird Folgendes angezeigt:

Name der Schnittstelle

Sie können den Namen ändern, indem Sie "Eigenschaften" auswählen und den Namen ändern.

IP-Adresse

Der Wert, der in den TCP/IP-Eigenschaften der Schnittstelle eingegeben ist. Falls die Schnittstelle so eingestellt ist, dass die IP-Adresse vom DHCP-Server abgerufen wird, sehen Sie die tatsächliche IP-Adresse, die der Schnittstelle zugewiesen wurde.

NAT “Ein” oder “Aus” (Aus)

Falls NAT so eingestellt ist, dass es an der Schnittstelle durchgeführt wird, so wird in dieser Spalte “Ein” angezeigt.

Paketfilterungs-Firewall

In diesem Abschnitt

Paketfilterung im Überblick

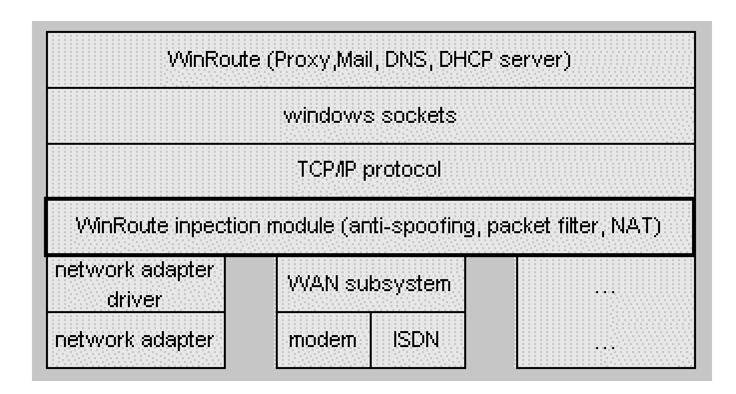
Das Herz einer jeden Firewall-Zugriffssteuerung ist selbstverständlich die Technik für die Zulassung bzw. Abweisung von Paketen an ein geschütztes Netzwerk. WinRoute verwendet eine der am häufigsten genutzten Techniken für die Steuerung der Netzwerkszugriffe: Paketfilterung. Andere Zugriffssteuerungen, wie beispielsweise ein integrierter Caching-Proxy-Server für HTTP-, FTP- und Gopher-Protokolle, sind primär als Elemente gedacht, die die ausgehende Leistung fördern sollen, und nicht als Sicherheitsfunktion.

Paketfilterung hat in der Branche für Sicherheitslösungen eine lange Tradition und wird noch immer häufig in Produkten wie im IOS Netzwerkbetriebssystem von Cisco eingesetzt. Bei ordnungsgemäßer Konfiguration können die Paketfilter sehr sicher gestaltet werden und sind besonders für viel frequentierte Internetseiten geeignet , da sie die besten Leistungsvorteile bieten.

Aufbau

Firewalls werden in der Regel auf verstärkte Plattformen gebaut, und die Software selbst ist normalerweise schwer zu umgehen. Eine der größten Schwächen bei vielen Netzwerksicherheitssystemen liegt jedoch in dem kurzen Zeitraum zwischen dem Zeitpunkt, an dem die Hardware aktiv in der Lage ist, den Datenstrom zu lenken, und dem Augenblick, in dem die Software die Kontrolle über die Netzwerkschnittstelle übernimmt. In diesem kritischen Moment kann die Sicherheit komplett gefährdet werden.

Der Treiber oder die Engine von WinRoute aktiviert sich, wenn die Kernroutinen des Windows Betriebssystems (der Kernel) sich selbst in den Speicher laden. Genauer gesagt lädt sich die Engine, bevor die NDIS- (Network Device Interface Specification-) Module geladen werden, so dass keine Verbindung unterstützt wird, bevor WinRoute aktiv ist. So ist der Schutz aller Schnittstellen aktiv, bevor schädlicher Datenverkehr oder andere Angriffe das System beeinträchtigen können. Dies ist eine positive Eigenschaft im Vergleich zu Einzelprodukten zur Erkennung von Angriffen, die als Dienst funktionieren und erst aktiv werden, wenn das System hochgefahren ist.



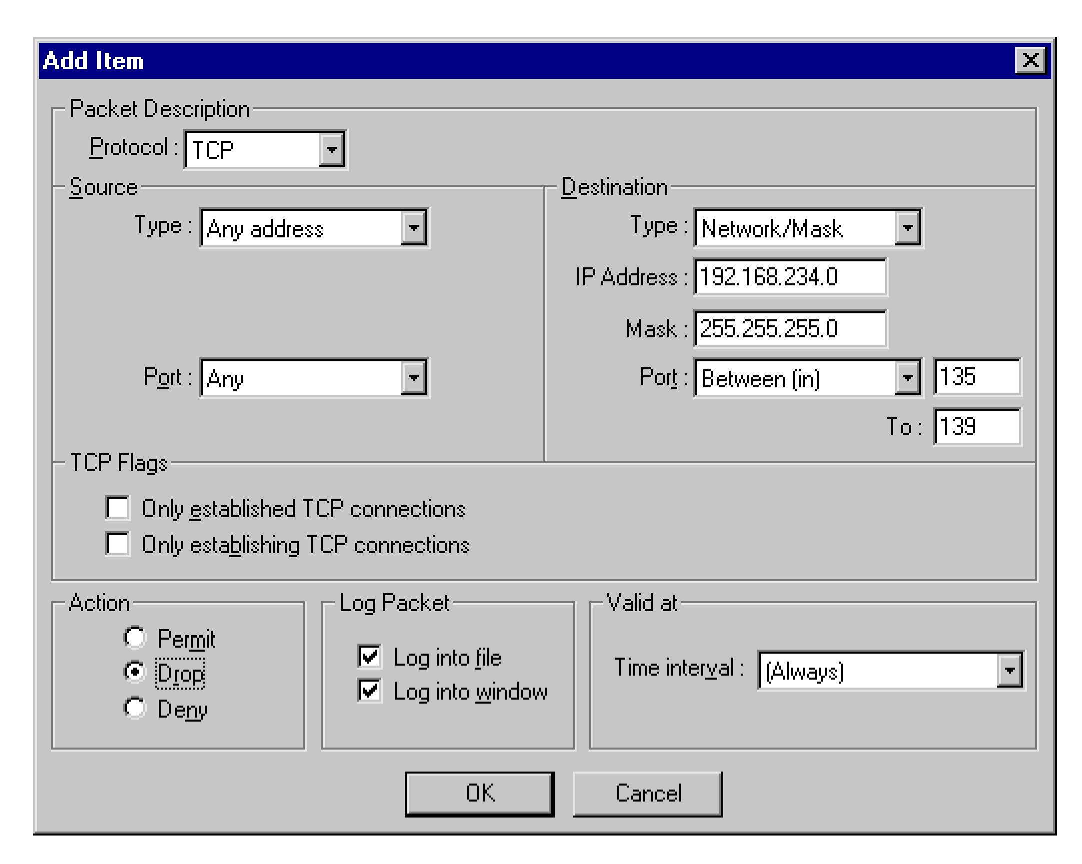
WinRoute "umschliesst" NDIS auf spezifische Weise, so dass der gesamte TCP/IP-Verkehr vom Treiber der Netzwerkkarte auf die Engine umgeleitet wird, bevor er zum Datenstapel (Stack) für die Netzwerkkommunikation des eigentlichen Betriebssystems gelangt.

Durch diese Funktion auf niedriger Ebene des Betriebssystems erhält die WinRoute-Engine eine einzigartige Kontrolle über den gesamten Netzwerkverkehr, der auf jeder Schnittstelle ankommt (egal, ob eingehend oder ausgehend). Wie es bei vielen Firewall-Produkten für Unternehmen der Fall ist (wie z. B. Check Point's Firewall-1), kann WinRoute die erste Entscheidung darüber treffen, ob einem bestimmten Paket Zugang gewährt wird oder nicht. Um es noch einmal hervorzuheben: Dies wehrt schädliche Angriffe gegen das Betriebssystem oder andere Software ab, die den von der Firewall angebotenen Schutz umgehen könnten. Dies ist mit Sicherheit wünschenswert bei Internet-Gateways, die über eine externe Verbindung verfügen, kann aber auch für Einzelrechner mit hohen Sicherheits- und Anonymitätsanforderungen wie Zugriffsüberwachungsanlagen von großem Nutzen sein. Software zur Zugriffsüberwachung wie Real Secure von Internet Security Systems (ISS) wäre auf einem von WinRoute geschützten Host praktisch unsichtbar.

Letztlich übernimmt die WinRoute-Engine die gesamte Weiterleitung der Kommunikation auf dem zu Grunde liegenden Betriebssystem (gleichgültig, ob es sich um Windows 9x, NT oder 2000 handelt). Dies garantiert, dass, falls aus irgendeinem Grund die WinRoute-Engine nicht richtig arbeitet, kein Datenverkehr zwischen den Netzwerken umgeleitet wird. Diese Sperrfunktion bei Ausfällen stellt seit vielen Jahren den traditionellen Standard für Firewall-Konfigurationen dar und dient dazu, private Netzwerke im Falle eines allgemeinen Systemausfalls zu schützen.

Regeln

Trotz der theoretischen Fragen, die die Paketfilterung betreffen, liegt die Hauptursache für eine Fehlfunktion eines modernen Firewall-Systems in der fehlerhaften Konfiguration. Dies ist insbesondere der Fall, wenn die mit der Administration betrauten Personen nicht genug Erfahrung mitbringen. WinRoute macht die Konfiguration von Filtern einfach und bietet dennoch ausreichend Flexibilität, so dass selbst unerfahrene Netzwerkadministratoren mit geringfügigen Kenntnissen über TCP/IP mit ein paar Mausklicks eine sichere Konfiguration erstellen können. Dies wird in der folgenden Bildschirmabbildung veranschaulicht.



Filterkriterien können pro Schnittstelle für alle der folgenden Einheiten festgelegt werden:

- eine einzelne IP-Adresse
- eine vom Administrator definierte Liste von IP-Adressen
- ein gesamtes Netzwerk oder Teilnetz

Beachten Sie, dass sowohl für den eingehenden als auch für den ausgehenden Datenverkehr Filter eingerichtet werden können.

Mit Hilfe dieser Funktionen ist die genaue Anpassung der Zugangsrichtlinien an die Sicherheitsanforderungen nahezu jedes Unternehmens möglich. Beispielsweise könnte einer Gruppe von Netzentwicklern der Zugang zu spezifischen externen Ressourcen gewährt werden, wie beispielsweise anonyme FTP-(Leitwerk-)Server, oder eine spezifische Liste interner Adressen für externe Partner-Netzwerke zugänglich gemacht werden, um elektronische Dateien abzulegen. Die eingehende/ausgehende Konfiguration ermöglicht den Schutz vor schädlichen internen Angriffen nach außen wie beispielsweise Back Orifice (BO) oder der verteilten Denial-of-Service (DDOS)-Servlets, die versuchen über unzuverlässige Protokolle nach draußen mit externen Angreifern zu kommunizieren.

Mit den Richtlinien kann der betreffende Datenverkehr entweder zugelassen, abgeworfen oder ablehnt werden. Beim Abwerfen werden nur die absolut notwendigen Informationen über die Firewall an den potenziellen Angreifer weitergegeben, da bei diesem Vorgang kein ICMP (Administrative Prohibited Filter) oder eine TCP- Zurücksetzen/Bestätigen-Anwort an ein TCP-SYN Paket gesendet wird (der erste Schritt in die standardmäßige Dreiwege-TCP-Handshake-Sequenz).

Diesen Richtlinien können verschiedene Prioritäten zugewiesen werden, so dass die ein- und ausgehenden Pakete in einer bestimmten, vom Benutzer definierten Reihenfolge bearbeitet werden. Die populärste dieser Einstellung beinhaltet so genannte "Bereinigungskriterien" in den Filterlisten, die den gesamten Verkehr blockieren, der von vorherigen Regeln, die über eine höhere Priorität in der Liste verfügten, nicht ausdrücklich genehmigt wurde. (Ein Beispiel für eine Bereinigungskriterium finden Sie im Kapitel zu den grundsätzlichen Filterkriterien in diesem Handbuch.)

Protokolle

Von WinRoute unterstützte Protokolle sind:

- Quell-IP
- sieben ICMP-Typen (oder alle)
- TCP
- UDP
- PPTP

Die Fähigkeit, ICMP-Quelltypen oder IP-Quellprotokolle zuzulassen oder zu blockieren, ist für Netzwerkadministratoren, die mit einer immer länger werdenden Liste von zu unterstützenden Anwendungsanforderungen konfrontiert sind, von unschätzbarem Wert. Besonders relativ neue VPN-Protokolle wie IPSec werden über IP-Protokolle 51 und 52 geleitet. Diese sind mit einem der eingeschränkteren Firewall-Produkte, die sich heute auf dem Markt befinden, nicht zu filtern, da sie nur auf TCP und UDP basierende Protokolle kontrollieren können.

Anti-Spoofing

Zusätzlich bietet WinRoute Anti-Spoofing-Funktionen (Funktionen zum Schutz vor elektronischer Täuschung), was verhindert, dass Pakete mit ungültiger Quelladresse innerhalb eines Netzwerks auftreten. Anti-Spoofing hätte die ICMP Smurf-Angriffe mit den verteilten Denial-of-Service-Angriffen auf so große Websites wie Yahoo und Buy.com, von denen im Februar 2000 berichtet wurde, verhindern können. WinRoute-Benutzer können durch diese Funktion beruhigt zurücklehnen, da sie wissen, dass ihre Netzwerke vor solchen Angriffen geschützt sind.

Protokolle und Paketanalyse

In diesem Abschnitt

Informationen zu den Protokollen und der Analyse

Eine wichtige Funktion jedes Sicherheitsproduktes ist die Fähigkeit, alle Vorgänge zu jedem Zeitpunkt in ausreichend detaillierter Form darzustellen. WinRoute listet sechs verschiedene Protokolle auf, einschließlich der Pakete, die das Netz passieren, der Benutzeraktivitäten, Filteraktionen und so weiter. Die einzelnen Protokolle werden in der folgenden Tabelle beschrieben:

HTTP-Protokoll	Zeigt nur HTTP-Daten an, die durch den Proxy-Server laufen; dies schließt IP-Quelladressen und Benutzernamen, die Zeitangabe, und HTTP-Anfragen und -Antworten ein.
Mail-Protokoll	Erfasst alle Aktivitäten des in WinRoute integrierten Mail-Servers, protokolliert SMTP (Simple Mail Transfer Protocol) und POP3 Sende- und Empfangsvorgänge.
Sicherheits- protokoll	Zeigt alle Aktivitäten an, die als "Protokollieren in Fenster/Datei" in den Paketfilterkriterien definiert werden. (Eine detaillierte Beschreibung der aufgeführten Produkte finden Sie weiter unten.)
Einwahl- protokoll	Protokolliert Nutzungsinformation für DFÜ-Schnittstellen, die von WinRoute überwacht werden.
Fehlerbehebungs- protokoll	Benutzerdefinierte Einstellungen, um alle ARP (Address Resolution Protocol), ICMP, UDP (User Datagram Protocol), TCP und/oder DNS (Domain Name Server)-Pakete, die physikalisch eine beliebige Schnittstelle des WinRoute-Routers passieren, zu protokollieren. Die genaue Konfiguration ist unter Einstellungen | Erweitert | Fehlerbehebungsinfo, Fehlerbehebung-Registerkarte.
Fehlerprotokoll	Zeigt alle nicht erfolgreichen Vorgänge, die in irgendeinem WinRoute-Modul auftreten.

Die Protokollierung kann auf der Konsole des WinRoute Administrator angezeigt werden, in eine Datei geschrieben werden oder beides. Die Protokolldateien werden unter \%installroot%\Logs gespeichert. Auf dieses Verzeichnis haben nur die NT/2000-Konten innerhalb von Administrator, Server-Operatoren, SYSTEM und der CREATOR OWNER, der WinRoute installiert hat, Zugriff.

Die Protokollinformationen, die von WinRoutes Sicherheitsprotokoll aufgezeichnet werden, sind kompakt und beinhalten alle notwendigen Daten, um eine angemessene Untersuchung möglicher schädlicher Vorgänge in die Wege zu leiten:

- Datum
- Zeit
- angewandtes Paketfilterkriterium
- Schnittstelle
- Aktion (Zulassen, Abgeben, Ablehnen)
- Protokoll
- IP-Quelladresse und TCP-Anschluss
- IP-Zieladresse und TCP-Anschluss

Der Test unter Bedingungen mit zu hoher Verkehrsdichte hat keinen Einfluss auf die Protokollierungsfähigkeit von WinRoute. Dies ist wichtig, um den Verlust wertvoller Daten sowie potenzielle Denial-of-Service-Situationen zu vermeiden, in denen die Firewall-Funktionsfähigkeit sich ausschaltet, wenn das Protokollierungssystem überlastet ist.

Fehlerbehebungsprotokoll

Das **Fehlerbehebungsprotokoll** ist das wichtigste Protokoll in WinRoute. Es ermöglicht Ihnen, **alle IP-Pakete** (TCP, UDP, ICMP, ARP, DNS) zu sehen, die eine der Schnittstellen im WinRoute-Computer tatsächlich passieren.

Im Fenster für die **Fehlerbehebungsereignisse** können Sie die Vorgänge sehen, die eventuell angezeigt werden sollen.

So lesen Sie das Protokoll

Von links nach rechts wird Folgendes angegeben:

Zeitangabe - Das Datum und der Zeitpunkt, zu dem der Vorgang stattfand oder das Paket die Schnittstelle passierte.

Das Protokoll - Der Protokolltyp des Pakets.

Von/An Schnittstellenname - Der Name der Schnittstelle und ob das Paket **an** die Schnittstelle gesendet wurde oder **von** der Schnittstelle kam. (Stellen Sie sich vor, dass WinRoute auf dem PC läuft, und die Schnittstellen als "Gates" zwischen dem Computer und dem Netzwerk fungieren).

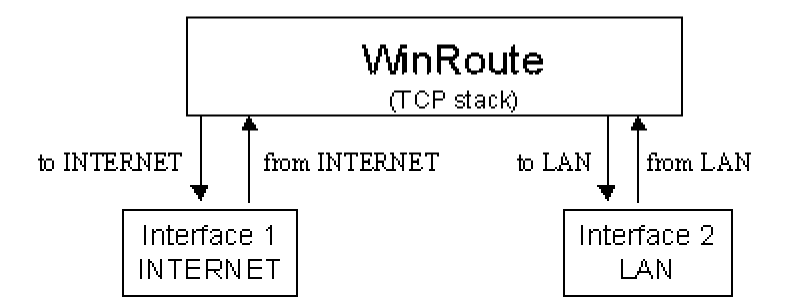
IP-Quelladresse -> IP-Zieladresse -Die "Quell-" und die "Ziel-" IP-Adresse, die im Paket enthalten ist.

Flag (Merker) - Weitere Angaben zum Vorgang.

Beispiel:

```
[10/Nov/1999 09:32:38] TCP: packet 511464, from lan,
length 1514, 192.168.1.7:2442 -> 192.168.1.1:25,
flags: ACK

[10/Nov/1999 09:32:38] TCP: packet 511465, to lan,
length 54, 192.168.1.1:25 -> 192.168.1.7:2442, flags:
ACK
```


WinRoute
(TCP stack)
to INTERNET
from INTERNET
to LAN
from LAN
Interface 1
INTERNET
Interface 2
LAN

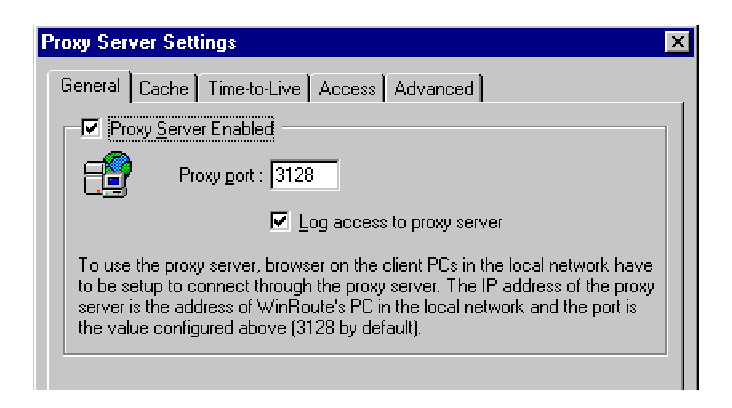
HTTP-(Proxy)-Protokoll

Das HTTP-(Proxy-)Protokoll ist ein leistungsstarkes Tool, das Ihnen dabei hilft, die Benutzeraktivitäten im Internet nachzuvollziehen. Es bietet benutzerfreundlichere Informationen über Benutzer, die auf das Internet zugreifen, als das Fehlerbehebungsprotokoll.

Wann funktioniert das Protokoll?

HTTP-(Proxy)-Protokoll zeigt nur Daten an, die über den PROXY-Server von WinRoute laufen. Das bedeutet, wenn Sie Daten vom PROXY-Server abrufen möchten, sollten Sie Ihre Benutzer dazu anhalten, über den PROXY-Server zu gehen. Weitere Informationen erhalten Sie im Kapitel über Firewall-Beispiele oder über den PROXY-Server.

Außerdem müssen Sie den Protokollzugang zur Konfiguration des Proxy-Server aktivieren.



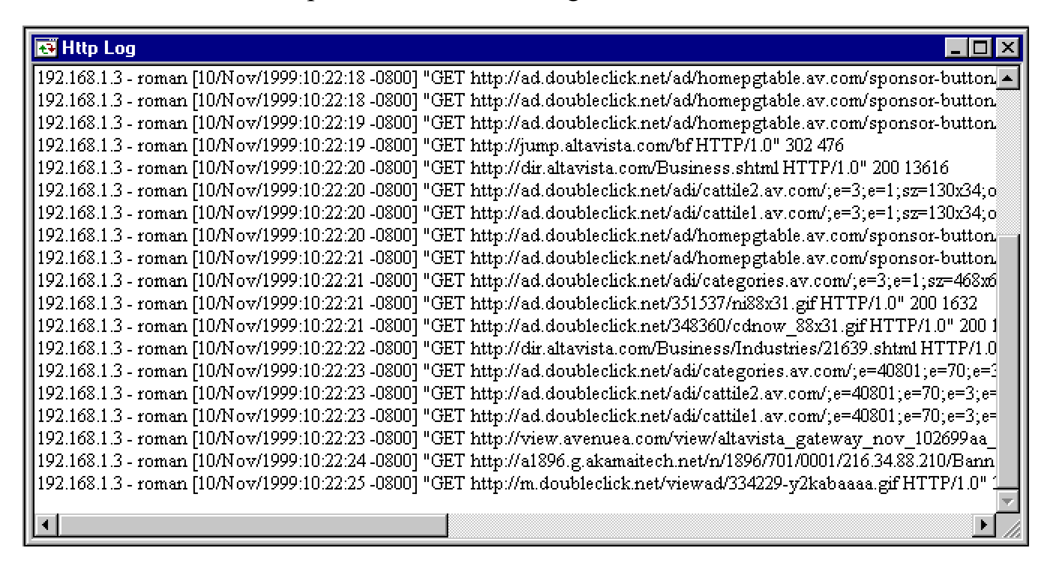
Wie wird das HTTP-(Proxy)-Protokoll gelesen?

```
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET
http://dir.altavista.com/Business.shtml HTTP/1.0" 200
13616
```

Von links nach rechts:

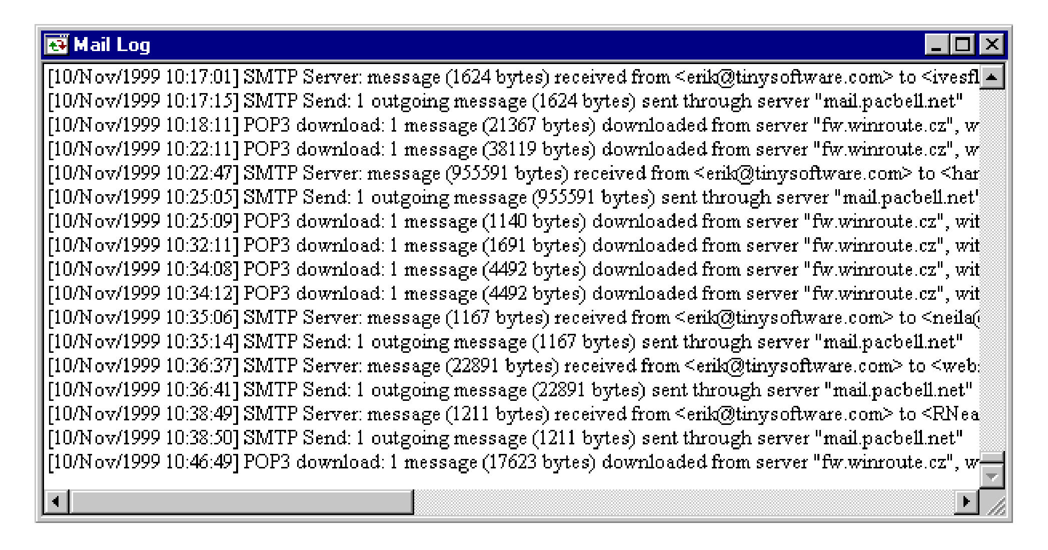
IP-Adresse - Name - Name und derzeitige IP-Adresse des Benutzers, der auf das Internet zugreift - Zeitangabe - Datum und Zeitpunkt des Zugriffs

ABRUFEN von "http..." - Das Ziel des Zugriffs



Mail-Protokoll

Das Mail-Protokoll führt alle Vorgänge des in WinRoute integrierten Mail-Servers auf. Sie können sehen, wie viele Nachrichten gesendet wurden, wie viele empfangen und an wen die Nachrichten gesendet wurden. Alle Vorgänge werden mit einer Zeitangabe versehen.



Fehlerprotokoll

Das Fehlerprotokoll zeigt alle nicht erfolgreichen Vorgänge in den aktiven WinRoute-Modulen an. Als Ergebnis können Sie die Fehler im Mail-Austausch, beispielsweise auf dem DNS-Server, sehen.

Error Log

```
[09/Nov/1999 09:54:07] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 09:56:23] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 09:58:38] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 09:59:14] mail: N:11001 - DNS query for "mail.pacbell.net" failed : host not found.
[09/Nov/1999 19:04:16] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 19:07:29] mail: G:0 - PASS command failed:
[09/Nov/1999 21:28:18] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 21:30:33] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 21:32:49] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 21:35:04] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 21:58:19] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[10/Nov/1999 03:16:09] mail: G:0 - PASS command failed:
[10/Nov/1999 05:41:04] mail: G:0 - USER command failed:
```

DHCP-Server

In diesem Abschnitt

DHCP im Überblick

In jedem Netzwerk muss das TCP/IP-Protokoll richtig konfiguriert sein. Das bedeutet, dass die IP-Adresse, die Netzwerkmaske, die Adresse des Standard-Gateways, die DNS-Serveradresse usw. an jedem Computer konfiguriert sein muss. Wenn die mit der Wartung betraute Person die Parameter für eine große Anzahl von Workstations manuell einrichten muss, lassen sich Fehler nur sehr schwierig vermeiden. Zu solchen Fehlern gehört beispielsweise die doppelte Vergabe einer Adresse, durch die es zu Kollisionen und Fehlfunktionen im Netzwerk kommen kann.

Dynamic Host Configuration Protocol (DHCP) ist eine WinRoute-Implementierung, mit der die Aufgabe der Netzwerkadministration vereinfacht werden soll. DHCP wird für eine dynamische Konfiguration des TCP/IP-Protokolls der Computer verwendet. Beim Start des Computers sendet der DHCP-Client eine Anfrage. Wenn der DHCP-Server eine Anfrage erhält, wählt er die Parameter zur TCP/IP-Konfiguration für den Client aus. Die Parameter umfassen die IP-Adresse, die Netzwerkmaske, den Standard-Gateway, die DNS-Serveradresse, die Domänenbezeichnung der Clients usw. Mit diesen Parametern erstellt der Server eine Antwort und sendet diese an den Client.

Der Server kann dem Client nur für eine begrenzte Zeit eine Konfiguration zuweisen (die so genannte Lease-Zeit). Der Server weist die IP-Adresse immer so zu, dass sie nicht mit einer anderen Adresse kollidiert, die über den DHCP-Server einem anderen Client zugewiesen wurde.

Ist ein DHCP-Server verfügbar, reicht es aus, die Option "IP-Adresse automatisch beziehen" zu aktivieren, damit der Server für eine angemessene Konfiguration der TCP/IP an den Workstations sorgt. Dies kann die Kosten für die Wartung des Netzwerks und die Organisation beträchtlich senken.

➢ ***Wenn einige Computer in Ihrem Netzwerk nicht dynamisch mit DHCP konfiguriert, sondern fest konfiguriert sind, müssen Sie sicherstellen, dass die von DHCP verwendeten Parameter nicht mit denen der festen Konfiguration kollidieren.***

DNS-Forwarder

In diesem Abschnitt

DNS-Weiterleitung

Jeder mit dem Internet verbundene Computer ist durch eine einzigartige, numerische IP-Adresse identifiziert. Um einen Computer im Internet zu erreichen, muss diese IP-Adresse dem Computer, der die Verbindung herstellt, bekannt sein. Da es zu umfangreich ist, IP-Adressen im Speicher zu behalten, wurde der Domain Name Server entwickelt.

Der DNS (Domain Name Server) ist eine Datenbank mit Namen, die sich leichter einprägen lassen als IP-Adressen. So muss der Benutzer die IP-Adresse des Servers, mit dem er/sie kommunizieren will, nicht kennen. Es reicht aus, den richtigen Namen einzugeben (z.B. www.yahoo.com) und der DNS wird die tatsächliche IP-Adresse finden.

DNS-Weiterleitung in WinRoute

WinRoute ist mit einem DNS-Modul ausgestattet, das in der Lage ist, DNS-Anfragen an einen ausgewählten DNS-Server im Internet weiterzuleiten. Das DNS-Modul speichert die Ergebnisse der Anfragen im internen Cache, wo sie für eine gewisse Zeit aufbewahrt bleiben. Nachfolgende, wiederholte Anfragen werden dann unter Verwendung der im Cache gespeicherten Daten beantwortet, ohne dass darauf gewartet werden muss, dass die Antwort aus dem Internet eingeht.

WinRoute ist in der Lage, DNS-Anfragen entsprechend der vom Benutzer definierten HOSTS-Datei zu beantworten. Nachdem eine DNS-Anfrage eingeht, sieht WinRoute zunächst in der HOSTS-Datei nach, bevor die DNS-Anfrage in das Internet weitergeleitet wird. Wird der entsprechende Eintrag gefunden, wird die Anfrage gemäß ihres Wertes beantwortet, wenn nicht, wird sie an den DNS-Server des Internets weitergeleitet.

PROXY-Server

In diesem Abschnitt

Proxy im Überblick

Der **hauptsächliche Zweck** eines Proxy-Servers ist es, die **Bandbreite** ihrer Internet-Verbindung durch Speicherung der passierenden Daten zu **erhöhen.** Falls die Benutzer auf das Internet über einen Proxy-Server zugreifen, kann der Proxy-Server die verschiedenen nachgefragten Objekte teilweise aus einem **Cache beantworten** (wie HTML-Seiten, Bilder und andere Arten von Dateien).

Dies **verringert** die Datenlast für die Internetverbindung und "erhöht" damit die Bandbreite für andere Benutzer. Zudem nimmt der gesamte Vorgang weniger Zeit in Anspruch als nötig wäre, um die Bilder nochmals vom Internet herunterzuladen.

Auf der anderen Seite verlieren die in einem Cache gespeicherten Objekte eines Proxy-Servers an Aktualität. Sie müssen die **TTL** (Time-To-Live, Paketlebensdauer) der gespeicherten Dokumente vergleichen, um Missverständnisse zu vermeiden, die daraus entstehen, dass Sie beispielsweise gerade die CNN-Nachrichten vom Vortag gelesen haben.

Schnellinstallation

Mit WinRoute ist für den Internetzugang **kein** Proxy-Server **erforderlich**. Ihre Internetverbindung wird über einen in WinRoute integrierten **NAT-Router** bereitgestellt. NAT ist weitaus besser für den gemeinsamen Internetzugriff geeignet als die Proxy-Server-Technik. Dennoch umfasst WinRoute auch einen Proxy-Sever, um die Caching-Funktion anzubieten, wenn erforderlich.

Um den Proxy-Server in WinRoute verwenden zu können, führen Sie folgende Schritte aus:

1 Im Menü von WinRoute Administration wählen Sie *Einstellungen -> Proxy-Einstellungen -> Allgemein*-Registerkarte. Aktivieren Sie die Option "Proxy-Server aktiviert". Behalten Sie den ursprünglichen Anschluss Nummer 3128 bei.



2 Gehen Sie in Ihrem Internet-Browser (Explorer, Netscape, Opera...) zu den Proxy-Einstellungen. Wählen Sie die manuelle Proxy-Konfiguration aus, und geben Sie die PC-Adresse des WinRoute Computers als Proxy-Server-Adresse für HTTP-, FTP- und Gopher-Protokolle ein. Geben Sie nun 3128 als Proxy-Anschlussnummer für alle Protokolle ein.

3 Testen Sie die Installation, indem Sie mit dem Browser auf eine beliebige Website zugreifen.

Registerkarte "Allgemeine Eigenschaften"

Proxy-Server aktiviert.

Mit dieser Option schalten Sie den Proxy-Server ein und aus.

Anschlussnummer

Die Anschlussnummer, die der Proxy-Server auf Anfrage überwacht. In der Regel ist es nicht erforderlich, die Anschlussnummer 3128 zu ändern.

Protokollzugang zum Proxy-Server

Wenn diese Option aktiviert ist, werden alle URLs, die vom Proxy über die Browser angefragt werden, in ein Protokoll aufgenommen.

Benutzer-Zugriffsüberwachung

Der Proxy-Server von WinRoute ermöglicht es dem Administrator, den Zugriff auf Internetseiten zu überwachen. Der Administrator kann festlegen, den Zugriff auf bestimmte Internetseiten oder Domänen nur für gewisse Benutzer und/oder Benutzergruppen zu gewähren.

Halten Sie die Benutzer dazu an, den Proxy-Server zu verwenden.

Wenn Sie die Zugriffsüberwachung des Proxys verwenden möchten, müssen Sie auch den direkten Zugriff auf Internetseiten sperren, so dass der Zugang über den Proxy die einzige verbleibende Alternative zum Internet-Browsing darstellt. Um den direkten Zugriff zu sperren, legen Sie ein Paketfilterkriterium fest. Weitere Informationen zur Paketfilterung finden Sie im Abschnitt über ***Paketfilter*** (see "So veranlassen Sie die Benutzer dazu, den Proxy-Server zu verwenden" on page 127) in diesem WinRoute-Benutzerhandbuch.

Konfiguration der Proxy-Zugriffsüberwachung

Um die Proxy-Zugriffsüberwachung von WinRoute zu konfigurieren, rufen Sie in den Proxy-Server-Einstellungen die Registerkarte "'Zugriff" auf.

Zugriffsliste

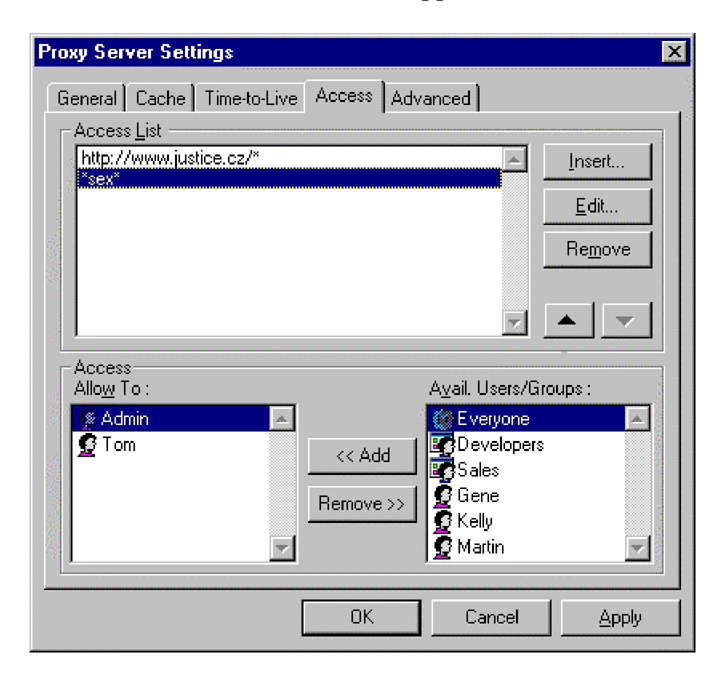
Die Liste der eingeschränkten URLs. Sie können Sternchen als Platzhalter im URL verwenden. Um alle Computer in irgendwo.com zu erfassen, können Sie beispielsweise die Zeichenfolge "*irgendwo.com" verwenden. WinRoute 4.0 setzt einen Test für Teilzeichenfolgen ein, um die URLs in Übereinstimmung zu bringen. So erhält man beispielsweise eine Übereinstimmung für die Zeichenfolge "sex" , die der gleichen Reihe von URLs entspricht wie die Zeichenfolge "*sex*" (nur die letztgenannte Variante wurde in der vorherigen Version von WinRoute unterstützt).

Zugriff genehmigt

Die Liste von Benutzern und/oder Benutzergruppen, die Zugang zu dem entsprechenden URL haben.

Verfügare Benutzer/Gruppen

Die Liste von Benutzern und Gruppen, die in WinRoute festgelegt sind.



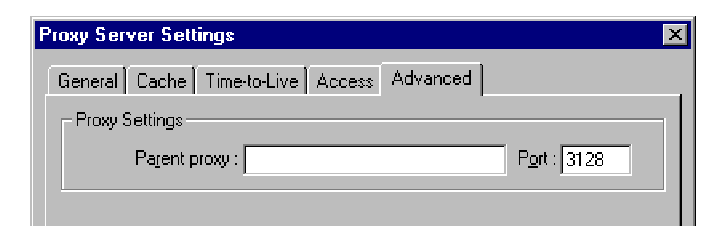
Wenn ein Benutzer versucht, auf eine Webseite zuzugreifen, deren Zugriff beschränkt ist, wird der Benutzer von seinem Browser dazu aufgefordert, eine Echtheitsbestätigung zu liefern. WinRoute wird überprüfen, ob der Benutzername und das Kennwort korrekt sind und ob dem Benutzer der Zugriff auf die bestimmte Internetseite erlaubt wurde.

Der Browser speichert den Benutzernamen und das Kennwort im Speicher. Alle nachfolgenden Anfragen bezüglich der Echtheitsbestätigung werden automatisch beantwortet, so dass der Benutzer den Namen und das Kennwort nicht noch einmal eingeben muss.

Auf der anderen Seite sollte der Benutzer sich dieser Funktion bewusst sein. Wenn Sie Ihren Benutzernamen und das Kennwort zu irgendeinem Zeitpunkt der Browser-Sitzung eingegeben haben, sollten Sie den Browser ausschalten, wenn Sie nicht mehr mit dem Computer arbeiten, um die von Ihnen zur Echtheitsbestätigung eingegebenen Daten aus dem Speicher zu löschen.

Erweiterte Eigenschaften

Auf der Registerkarte "Erweitert" der Proxy-Server-Einstellungen können Sie WinRoute so einrichten, dass ein Parent-ROXY-Server verwendet wird.



Mitunter werden Sie Zugang zu einem PROXY-Server haben, der über einen sehr **großen Cache** oder eine **schnelle** Internet-Verbindung verfügt. Ihre Verbindung zu diesem Server wird dann auch ziemlich schnell sein, zumal vielleicht neben dem von Ihnen für Ihre eigene Internetverbindung verwendeten Link ein zusätzlicher Link genutzt wird.

Um Ihren Datendurchsatz zu verbessern, können Sie festlegen, dass der WinRoute-Proxy alle Anfragen an den Parent-PROXY-Server weiterleitet. Um dies zu tun, geben Sie einfach den Namen dieses **Parent-Proxys** sowie die Anschlussnummer in das entsprechende Feld in der Registerkarte "**Erweitert**" ein.

Informationen zum Cache-Speicher

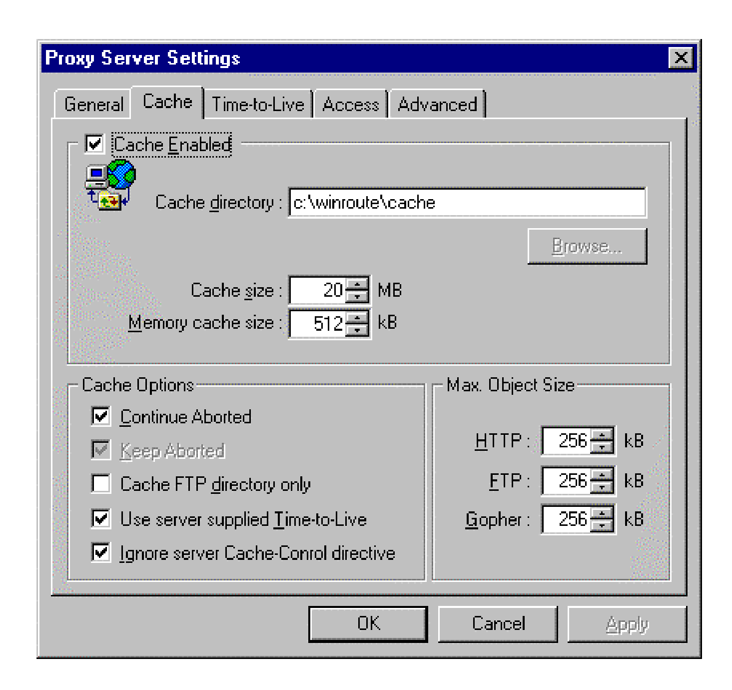
Der WinRoute Proxy-Server speichert Daten auf eine **sehr sparsame** Art und Weise. Alle zwischengespeicherten Objekte werden in **einer Datei von festgelegter Größe** gespeichert. Im Gegensatz hierzu speichern viele Proxy-Server in der Regel jedes Objekt in eine separate Datei.

Falls die Festplatte **große Zuordnungseinheiten** (wie FAT16) verwendet, resultiert daraus eine **beträchtliche Verschwendung** von Festplattenspeicherplatz, weil viele Komponenten von Internetseiten sehr klein sind. Normalerweise sind 50 % der Objekte kleiner als 6 Kilobyte, wohingegen die Größe der Zuordnungseinheiten auf einer großen Festplatte 32 KB beträgt (durch das Dateisystem der FAT = File Allocation Table).

Durch die Tatsache, dass der WinRoute-Cache Daten in einer einzelnen Datei speichert, wird viel Festplattenspeicherplatz gespart, da sich alle zwischengespeicherten Objekte in einer Datei befinden. Im Vergleich zu der üblichen Vorgehensweise sind weniger als 10% des Speicherplatzes erforderlich. Dies bedeutet, dass Sie weniger Festplattenspeicherplatz benötigen oder den gleichen Speicherplatz viel effizienter nutzen können.

Auf Grund der einzelnen Datei mit festgelegter Größe kann WinRoute sehr effiziente Index-Techniken verwenden, die die Geschwindigkeit des Cache von WinRoute erhöhen.

Cache -Einstellungen



Cache aktiviert

Schaltet die Cache-Funktion ein und aus. Falls nicht aktiv, wird jede Internetseite immer direkt aus dem Internet abgerufen.

Cache-Verzeichnis

Das Verzeichnis, in dem die Daten zwischengespeichert werden.

Cache-Größe

Die Größe des Festplattenspeicherplatzes, der vom Proxy-Cache verwendet wird. Berücksichtigen Sie beim Festlegen der Größe unter anderem die Anzahl der Benutzer sowie den von diesen verursachten Datenverkehr. Wenn Sie über genügend freien Speicherplatz verfügen, können Sie einen größeren Cache installieren. Die maximale Größe beträgt 3072 MB (3 GB).

Abgebrochen fortsetzen

Falls aktiv, wird der PROXY-Server immer das Herunterladen eines Objektes aus dem Internet abschließen, auch wenn der Browser des Benutzers die Anfrage abbricht (der Benutzer klickt auf die Schaltfläche "Stopp" oder folgt einem Link auf eine andere Seite ohne abzuwarten, bis die aktuelle Seite vollständig heruntergeladen ist). Bei nachfolgenden Besuchen der gleichen Seite erfolgt der Aufbau wesentlich schneller.

Abgebrochen behalten

Mit dieser Funktion wird der WinRoute-PROXY-Server beauftragt, auch unvollständige Objekte zwischenzuspeichern (Internetseiten, Bilder). Dies führt zumindest zu einer teilweisen Beschleunigung, wenn die Webseite erneut besucht wird. Wenn "Abgebrochen fortsetzen" aktiviert ist, wird die Einstellung "Abgebrochen behalten" ignoriert.

Nur Cache-FTP-Verzeichnis

Beim Durchsuchen von FTP-Servern können Sie diese Option verwenden, um nur die Verzeichniseinträge zwischenzuspeichern. Wenn Sie auch die Dateien, die vom FTP-Server heruntergeladen wurden, speichern möchten, deaktivieren Sie diese Option. Die Entscheidung, ob eine bestimmte Datei zwischengespeichert wird, hängt auch von der Größe ab (siehe "Max. Objektgröße" unten).

Server mit Time-to-Live verwenden

Time-to-Live ist der Zeitraum, nach dem eine bestimmte Webseite als veraltet angesehen wird und ihr Inhalt vom Server erneut aufgerufen werden muss. Diese Option instruiert den WinRoute-Proxy-Server, die Time-To-Live (TTL) einzuhalten, die mit den einzelnen Seiten einhergeht. Falls eine Seite nicht über eine TTL verfügt, wird die Standard-TTL des Proxys verwendet.

Server-Anweisung zur Cache-Steuerung ignorieren

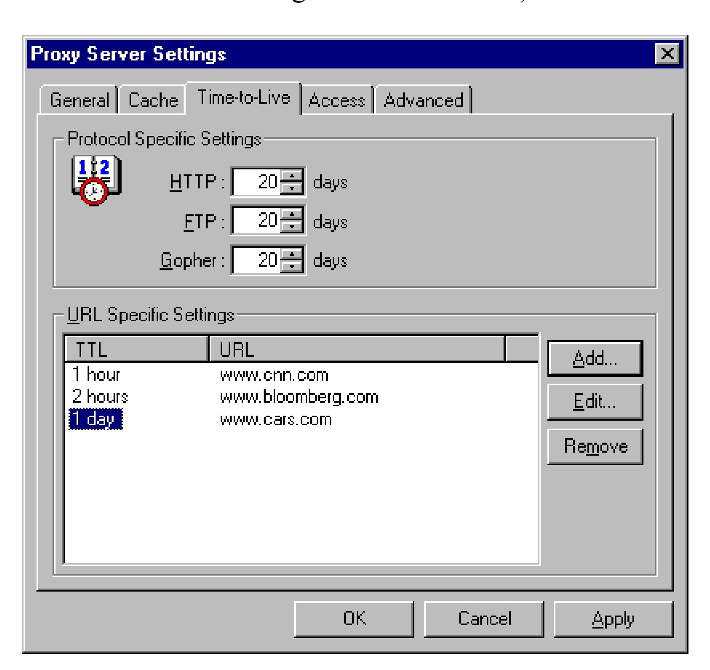
Falls die Inhalte einer Webseite sich sehr oft ändern, wird der Autor sich dazu entschließen, die Anweisung "kein Cache" für diese Seite setzen. Dies ist eigentlich eine sehr nützliche Funktion. Allerdings verwenden manche Internetseiten diese Anweisung viel zu oft, manchmal für alle Seiten, und eliminieren damit den Zweck des Proxy-Servers. Wenn Sie sich dagegen schützen müssen, aktivieren Sie diese Option.

Maximale Objektgröße

Die maximale Größe des zu speichernden Objekts im Cache. Größere Objekte werden an den Browser des Benutzers weitergeleitet, aber nicht in den Cache aufgenommen. Normalerweise müssen Sie große Objekte (wie Programm-Archiv-Dateien) nicht zwischenspeichern, da Sie diese nicht wiederholt herunterladen.

Time-to-Live

Sie können TLL-Standardwerte (Time-To -Live) festlegen, falls für eine Internetseite keine TTL definiert wurde oder falls Sie die vom Server gelieferten TTL-Werte ignorieren möchten (siehe die Option "Server mit Time-to-Live verwenden" auf der Registerkarte "Cache").



Protokollspezifische Einstellungen

Hier können Sie die Standard-Time-to-Live in Tagen für die HTTP-, FTP- und Gopher-Protokolle einstellen.

URL-spezifische Einstellungen

Wenn Sie individuelle Time-to-Live-Werte für einige Domänen, Web-Server oder individuelle Seiten festlegen möchten, geben Sie die einzelnen URLs hier ein. Sie können die TTL in Tagen und/oder Stunden festlegen.

Sie können Sternchen als Platzhalter im URL verwenden. Als neue Funktion von Winroute wird ein Test für Teilzeichenfolgen durchgeführt, um die Übereinstimmung mit den URLs zu prüfen. Sie können einfach "ftp" eingeben, um alle Server zu erhalten, die "ftp" im Namen tragen. Vorher mussten Sie "*ftp*" eingeben, um diesen Fall mit einzubeziehen.

Wir möchten Sie darauf hinweisen, dass wenn Sie "Server mit Time-to-Live verwenden" auf der Registerkarte "Cache" aktiviert haben, die vom Server gelieferte TTL über eine höhere Priorität verfügt als "URL-spezifische Einstellungen".

So veranlassen Sie die Benutzer, Proxy anstelle von NAT zu verwenden

Auch wenn **NAT** Ihnen eine ausgezeichnete Internet-Verbindungsfähigkeit verleiht, möchten Sie möglicherweise manchmal, dass die Benutzer den **Proxy-Server** verwenden, um auf das **World Wide Web** zuzugreifen. Dies ist beispielsweise der Fall, wenn Sie für das gesamte Unternehmen eine 56 KB-Leitung zum Internet haben und dafür der Cache sehr nützlich wird, oder wenn Sie **den Benutzer- Zugriff** anhand eines integrierten **URL-Filters** überwachen möchten.

Um mit einem Proxy auf das Internet zuzugreifen, müssen Sie alle Browser so einstellen, dass diese den PROXY-Server verwenden. Denken Sie daran, dass der Standardanschluss des PROXY-Servers **3128** ist. Bei Bedarf können Sie den Anschluss ändern. Die Benutzer können den Proxy umgehen und direkt über NAT auf das Internet zugreifen. Um dies zu vermeiden, müssen Sie die Firewall entsprechend einrichten. Ein Beispiel hierzu finden Sie im Kapitel über ***Firewall-Einstellungen*** (see "So veranlassen Sie die Benutzer dazu, den Proxy-Server zu verwenden" on page 127).

So verwenden Sie den Parent-Proxy-Server

Parent-Proxy-Server

In manchen Fällen, müssen Sie den WinRoute-Server mit einem übergeordneten Proxy-Server verbinden, dem so genannten **Parent- Proxy**. Gehen Sie in das Menü *Einstellungen/Proxy-Server*, wählen Sie die Registerkarte *Erweitert* aus, und geben Sie hier die IP-Adresse und den Anschluss ein.



Parent-Proxy-Benutzername und -Kennwort

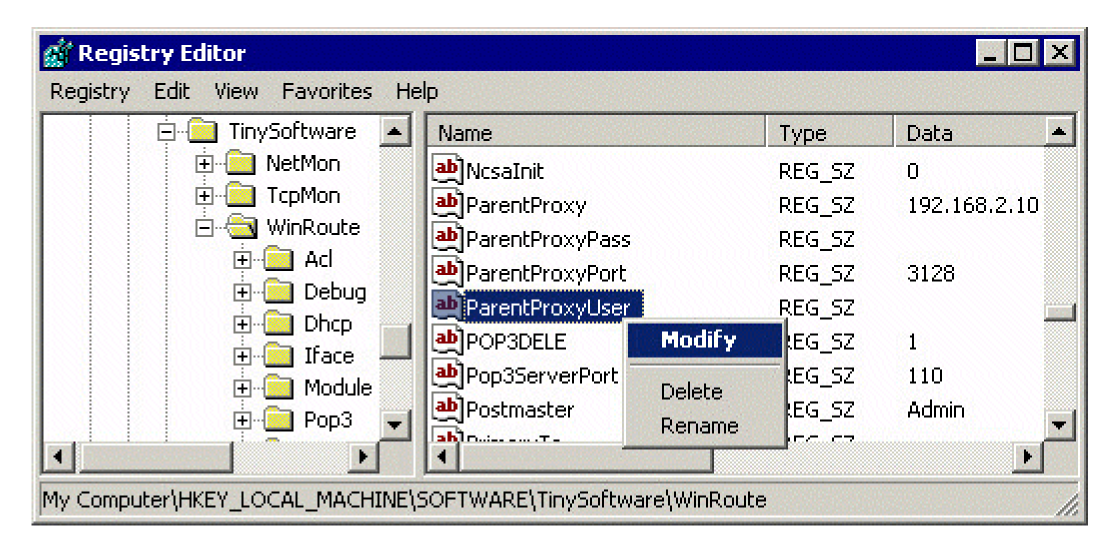
Möglicherweise wird der Benutzer vom Parent-Proxy-Server aufgefordert, eine Autorisierung einzugeben, um ähnlich wie bei WinRoute auf bestimmte (oder alle) Internetseiten zugreifen zu können (Einzelheiten finden Sie im Kapitel *Proxy Zugangskontrolle*). WinRoute Pro 4.1 schließt eine solche Autorisierung ab Build 22 mit ein.

So richten Sie eine Autorisierung ein:

- Halten Sie die WinRoute Engine an (von den Windows-Diensten aus oder mit dem Monitorprogramm der WinRoute Engine)
- Starten Sie Windows Registry Editor (regedit.exe)
- Suchen Sie den Schlüssel *HKEY_LOkAL_MACHINE\Software\TinySoftware\WinRoute*
- Im rechten Feld finden Sie die Textfelder **ParentProxyUser** und **ParentProxyPass**, und ändern Sie deren Inhalt in den entsprechenden Benutzernamen und das Kennwort.

- Schließen Sie den Registry Editor und starten Sie die WinRoute Engine.

Nach Abschluss dieses Vorgangs autorisiert sich der Proxy-Server von WinRoute selbst als Parent-Proxy-Server.



MAIL-Server

In diesem Abschnitt

Der MAIL-Server von WinRoute

WinRoute verfügt über einen SMTP/POP3-MAIL-Server mit allen Funktionen. Sie können diesen auf gleiche Weise nutzen wie den MAIL-Server Ihres Internet-Diensteanbieters (ISP). Der MAIL-Server von WinRoute ermöglicht es Ihnen, E-Mails in das Internet sowie an lokale Benutzer innerhalb Ihres LAN zu versenden. Es ist auch möglich, E-Mails zu erhalten und diese in den Mailboxen der Benutzer von WinRoute zu speichern. WinRoute beinhaltet auch einen Terminplaner, mit dem Sie Ihren E-Mail-Austausch zeitlich planen können.

Wenn Sie den MAIL-Server nicht verwenden

Sie müssen den MAIL-Server nicht verwenden. Sie können weiterhin den MAIL-Server Ihres Internetdiensteanbieters oder einen anderen MAIL-Server einsetzen. In diesem Falle fungiert WinRoute als Router/Firewall, der es Ihrer E-Mail-Client-Software ermöglicht, mit dem E-Mail-Server Ihres Internetdiensteanbieters zu kommunizieren.

- ***Hinweis! Stellen Sie Ihre E-Mail-Client-Software nicht so ein, dass sie den Proxy verwendet! Sie müssen die NAT von WinRoute für den Zugriff auf das Internet verwenden und Ihre Client-Software so einstellen, dass sie direkten Zugang zum Internet hat. Falls es Ihnen nicht möglich ist, den Austausch von E-Mails einzurichten, bedeutet dies, dass NAT nicht richtig konfiguriert ist. In der nachfolgenden*** Checkliste ***finden Sie nähere Informationen zur richtigen Konfiguration von NAT.***

Benutzerkonten

In diesem Abschnitt

Informationen zu den Benutzerkonten

WinRoute - Benutzerkonten

WinRoute kann mit individuellen Benutzerkonten, die gruppiert werden können, programmiert werden (konfiguriert unter Einstellungen | Konten… | Benutzer). Bereits vorhandene Benutzer von Windows NT/2000 können auf der Registerkarte "Erweitert" unter "Einstellungen | Konten… Menü" importiert werden.

Benutzer

Als Benutzer von WinRoute können Sie an der Verwaltung von WinRoute teilnehmen, über eine Mailbox verfügen und die Kriterien für die Zugangsbeschränkungen über den WinRoute-Proxy mitbestimmen.

Benutzer können Gruppen erstellen und diesen die oben genannten Privilegien oder Einschränkungen erteilen.

Hinzufügen eines Benutzers

Führen Sie folgende Schritte aus, um einen Benutzer hinzuzufügen:

1 Rufen Sie das Menü **Einstellungen->Konten** auf.

2 Aktivieren Sie die Schaltfläche **Hinzufügen.**

3 Legen Sie **Benutzernamen** und **Kennwort** fest.

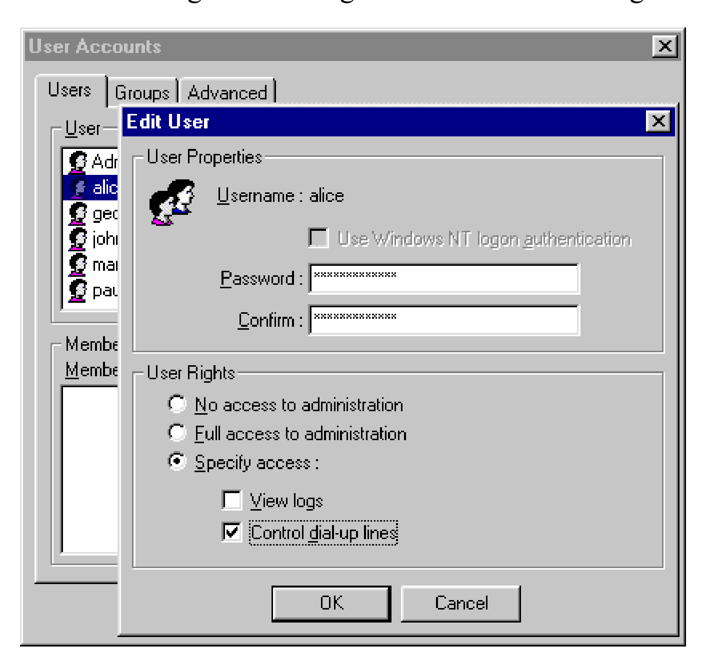
4 Weisen Sie Benutzern **Rechte** zu:

Der Benutzer hat kein Recht, WinRoute zu verwalten.

Der Benutzer verfügt über Vollzugriff auf das Verwaltungsprogramm.

- **Ansichtsprotokoll:** Der Benutzer hat das Recht, sich bei WinRoute Administrator anzumelden und nur die Protokollfenster einzusehen (Fehlerbehebungsinformationen, Proxy-Protokoll, Mail-Protokoll usw.). Der Benutzer besitzt keine darüber hinausgehenden Zugriffsrechte zur Änderungen von anderen Einstellungen.

- **Einwahlverbindungen kontrollieren:** Der Benutzer hat das Recht, sich bei WinRoute Administrator anzumelden und die Internetverbindung einzurichten bzw. zu unterbrechen. Der Benutzer besitzt keine darüber hinausgehenden Zugriffsrechte zur Änderung von anderen Einstellungen.



Benutzergruppen

In WinRoute können Sie Benutzer verschiedenen Gruppen zuweisen. Ein Benutzer kann gleichzeitig Mitglied mehrerer Gruppen sein.

Sie können diesen Gruppen **Rechte** zuweisen.

➢ ***Hinweis: Die einer Gruppe zugewiesenen Rechte "überschreiben" die Rechte, die dem einzelnen Benutzer zugewiesen wurden.***

Mitglieder der Gruppe können über folgende **Rechte** verfügen:

Der Benutzer hat kein Recht, WinRoute zu verwalten.

Der Benutzer hat Vollzugriff auf das Verwaltungsprogramm.

- **Ansichtsprotokoll:** Der Benutzer hat das Recht, sich bei WinRoute Administration anzumelden und nur die Protokollfenster einzusehen (Fehlerbehebungsinformationen, Proxy-Protokoll, Mail-Protokoll usw.). Der Benutzer besitzt keine darüber hinausgehenden Zugriffrechte zur Änderung von anderen Einstellungen.
- **Einwahlverbindungen kontrollieren:** Der Benutzer hat das Recht, sich bei WinRoute anzumelden und die Internetverbindung einzurichten bzw. zu unterbrechen. Der Benutzer besitzt keine darüber hinausgehenden Zugriffsrechte zur Änderung von anderen Einstellungen.

Fernverwaltung

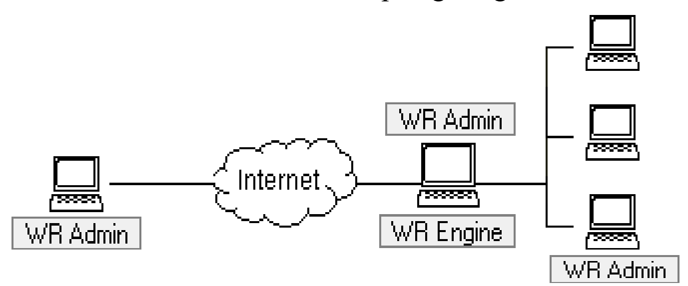
WinRoute Pro bietet den Benutzern den Vorteil der Fernverwaltung. Mit den entsprechenden Einstellungen ist es möglich, Ihre Firewall von jedem Ort der Welt aus sicher zu verwalten. Der Zugang zur Engine wird durch eine komplizierte Verschlüsselung und ein Kennwort gesichert.

WinRoute Pro-Komponenten

WinRoute Pro 4.x besteht aus drei Modulen:

WinRoute Engine führt jede Weiterleitung und Analyse durch (NAT, Paketfilterung, Anschlusszuordnung usw.). Sie können die WinRoute Engine von WinRoute aus, oder wenn Sie mit WindowsNT arbeiten, direkt über die Option für die NT-Dienste starten und stoppen. WinRoute Engine wird unter Windows2000/NT/98 oder 95 unsichtbar als Dienst ausgeführt.

WinRoute Engine Monitor ist die Überwachungsanwendung, die anzeigt, ob die WinRoute Engine ausgeführt wird oder nicht. Sie wird durch das kleine blaue Symbol unten rechts auf dem Desktop angezeigt.



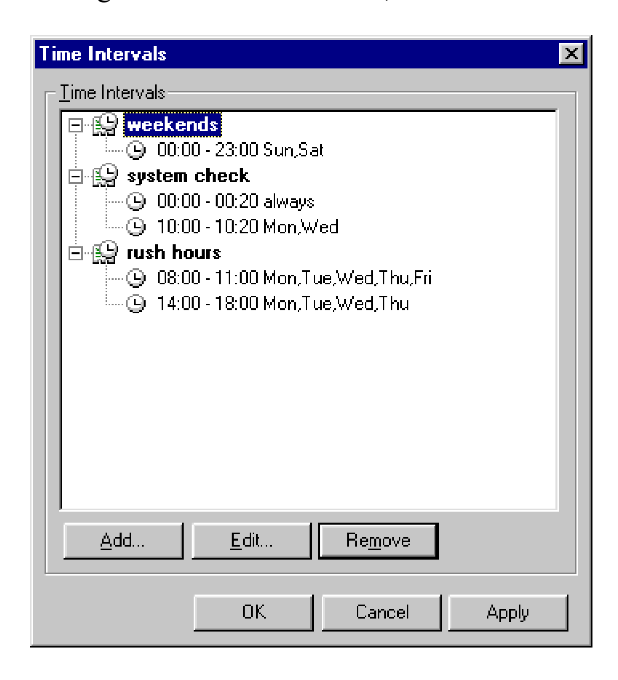
WinRoute Administrator liefert die Konfiguration und die Einstellungen für die WinRoute Engine. WinRoute Administrator ist eine separate Anwendung (wradmin.exe), die auf jedem Computer installiert und mit einer TCP/IP Verbindung an einen Computer mit WinRoute angeschlossen werden kann. Informationen über die Einstellungen, die für die WinRoute Engine notwendig sind, um einen Fernanschluss zu ermöglichen, finden Sie in den anderen Kapiteln dieses Abschnitts.

Zeitintervalle

Sie können Zeitzonen - vordefinierte Zeitintervalle - festlegen, um bestimmte Vorgänge auszuführen. Diese Vorgänge können sein:

- Paketfilterung
- E-Mail-Austausch (Senden und Empfangen)
- Verbindung zum Internet
- Erweiterte NAT-Einstellungen

Die Zeitzone ist eine Gruppe von Zeitintervallen. Es lässt sich so ein nicht-homogener Zeitraum erstellen, der aus verschiedenen Intervallen besteht.



➢ ***Beispiel: Sie können eine Zeitzone erstellen, die "Feiertage und Abende" genannt wird, und die Folgendes beinhaltet: Samstag, Sonntag, Montag von 16:00 Uhr bis 18:00, Dienstag von 17:00 bis 19:00.***

Führen Sie folgende Schritte aus, um die Zeitzone festzulegen:

1 Gehen Sie in das Menü *Einstellungen => Erweitert => Zeitintervalle*

2 Geben Sie der Zeitzone einen Namen.

3 Fügen Sie das neue Zeitintervall hinzu.

KAPITEL 2

INSTALLATION UND KONFIGURATION

In diesem Kapitel

Systemvoraussetzungen

Um WinRoute Pro 4.1 auszuführen, benötigen Sie Folgendes:

- Einen PC mit Pentium-Prozessor (Einfach- oder Dualprozessor)
- Windows 95/98/NT4.0/2000 Betriebssystem
- 32 MB Speicher
- davon 1 MB freier Speicherplatz
- Mindestens 2 verfügbare Schnittstellen. Diese können sein: Ethernet, RAS, TokenRing, DirecPC.

Checkliste

Für alle WinRoute-Benutzer gibt es eine Liste von Grundregeln und -einstellungen, die die erfolgreiche Anbindung Ihres Netzwerks mit dem Internet garantieren. Natürlich ist ein funktionsfähiger Internetanschluss dafür Voraussetzung.

Sie sollten die unten beschriebenen Einstellungen vornehmen, wenn Sie NAT für einen gemeinsamen Internetzugang nutzen möchten. Auch wenn Sie einen PROXY-Server (in WinRoute integriert) verwenden möchten, müssen Sie diese Einstellungen vornehmen. In diesem Fall müssen Sie Ihre Browser und Ihre Anwendungen auf den PROXY-Server von WinRoute ausrichten. Wir empfehlen dringend, NAT zu verwenden, wann immer dies möglich ist. Es geht schneller, ist sicherer und zuverlässiger.

Grundregeln und -einstellungen

1 **Auf dem WinRoute-PC - Zwei Schnittstellen (NICs)**
Vergewissern Sie sich, dass der WinRoute-Computer über (mindestens) zwei Schnittstellen verfügt. Eine für die Internetverbindung und eine für die lokale/Client-Verbindung. Diese können Netzwerkadapter oder RAS-Leitungen sein. Eine Schnittstelle (Ethernet oder RAS/DFÜ) wird für die Internetverbindung verwendet, wohingegen für die Verbindung zu Ihrem/n Netzwerk(en) (eine) andere Schnittstelle(n) benutzt wird/werden (Ethernet, Token Ring ...).

2 **Vergewissern Sie sich, dass alle IP-Adressen so eingerichtet sind, dass Pings gesendet werden können!** Damit WinRoute richtig ausgeführt wird, müssen die Client-Computer in der Lage sein, sowohl die öffentliche als auch die private IP-Adresse des Host-Computers von WinRoute zu pingen.

3 **Auf dem WinRoute-PC - Aktivieren Sie NAT an der Internetschnittstelle!**
Überprüfen Sie, dass NAT für die Schnittstelle zum Internet (Ethernet, RAS-Leitung) aktiviert ist. Stellen Sie dies im Menü **Einstellungen => Schnittstellentabelle** ein, und rufen Sie die Eigenschaften der gewünschten Schnittstelle auf.

4 Auf dem WinRoute-PC - Deaktivieren Sie NAT an der internen Schnittstelle!
Vergewissern Sie sich, dass NAT an der Schnittstelle oder den Schnittstellen zum internen Netzwerk **deaktiviert** ist.
Hinweis! In sehr speziellen Installationen kann NAT sogar an der internen Schnittstelle aktiviert bleiben. Falls verfügbar, sehen Sie hier ein Beispiel.

5 Auf dem WinRoute-PC - Kein Gateway an der internen Schnittstelle!
Vergewissern Sie sich, dass KEIN Standard-Gateway in den Netzwerkeigenschaften der Schnittstelle (Netzwerkkarte) zum internen Netzwerk vorhanden ist. Selbstverständlich wird der Standard-Gateway der Schnittstelle zum Internet gemäß den Angaben Ihres Internetdiensteanbieters eingestellt.

6 Auf dem WinRoute-PC - Geben Sie die Optionen bei der DHCP-Konfiguration ein!
In den meisten Fällen werden Sie den DHCP-Server von WinRoute zur automatisierten Konfiguration verwenden. Überprüfen Sie genau, dass Sie den/die Gültigkeitsbereich(e) der IP-Adressen, die Sie vom DHCP-Server zusammen mit den Optionen zugewiesen haben möchten, festgelegt haben. Geben Sie unter Optionen andere Daten, die an Ihre Workstations gesendet werden an (z. B. DNS-Server, Standard-Gateway usw.).

7 Auf dem Client-PC - WinRoute's interne IP-Adresse ist der Standard-Gateway!
Der WinRoute-PC fungiert als STANDARD-GATEWAY für alle Computer im LAN. Verwenden Sie daher die IP-Adresse der internen Netzwerkschnittstelle am WinRoute-Host (z. B.192.168.1.1) als Gateway an jedem internen oder Client-Computer. Geben Sie diesen Wert auf jedem "Client"-Computer ein, ODER geben Sie ihn einmal auf dem DHCP-Server von WinRoute ein. Der Server weist den Wert automatisch Ihren Workstations zu!
Wenn Sie einen anderen Standard-Gateway nutzen müssen, finden Sie weitere Informationen hierzu in den Beispielen für erweitertes (Inter-)Networking!

8 Auf dem Client-PC - Aktivieren Sie DNS!
In den meisten Fällen werden Sie die in WinRoute integrierte DNS-Weiterleitung als DNS-Server für Ihre Computer am Netz verwenden. Vergewissern Sie sich, dass die in WinRoute integrierte DNS-Weiterleitung IN BETRIEB und konfiguriert ist. Sie können die DNS-Serveradresse Ihres Internetdiensteanbieters verwenden, indem Sie diese direkt in die entsprechenden Felder der TCP/IP-Konfiguration jedes Netzwerkcomputers eingeben.

- ***Wenn WinRoute nur als Firewall oder MAIL-Server verwendet wird (d. h. ohne Anforderung hinsichtlich gemeinsamer Internetnutzung), ist es NICHT notwendig, NAT für eine Schnittstelle zu aktivieren.***

- ***Die Schnittstellen am WinRoute-Computer müssen verschiedene IP-Adressen von verschiedenen Netzwerken haben. In der Regel haben Sie eine lokale (LAN) Schnittstelle und eine Internetschnittstelle. In diesem Fall treten keine Probleme auf. Für den Fall, dass Sie drei Schnittstellen haben (2 lokale und eine Internetschnittstelle), sollten Sie den lokalen Schnittstellen IP-Adressen von unterschiedlichen Netzwerken zuweisen (eine 192.168.1.1 und die andere 192.168.2.1).***

Software-Konflikte

Hinsichtlich inkompatibler Software sind folgende Probleme bekannt:

Norton Antivirus

Deaktivieren Sie Anschluss 110 in der Norton Antivirus-Konfiguration, wenn Sie den MAIL-Server von WinRoute ausführen möchten. Wenn Sie Anschluss 110 in Norton aktiviert lassen, wird der Computer nicht gestartet.

WinGate

Deinstallieren Sie WinGate vor der Installation. Deinstallieren Sie sowohl die Server- als auch die Client-Software.

SyGate

Deinstallieren Sie SyGate vor der Installation. Deinstallieren Sie sowohl die Server- als auch die Client-Software.

MS Proxy Server

Deinstallieren Sie MS Proxy Server vor der Installation. Deinstallieren Sie sowohl die Server- als auch die Client-Software. Entfernen Sie das TCP/IP-Protokoll, starten Sie den Computer neu, und rufen Sie TCP/IP wieder auf.

Microsoft Internet Connection Sharing

Deinstallieren Sie MS ICS vor der Installation, entfernen Sie das TCP/IP-Protokoll, starten Sie den Computer neu, und rufen Sie TCP/IP wieder auf.

WinProxy von Ositis

Deinstallieren Sie WinProxy vor der Installation, entfernen Sie das TCP/IP-Protokoll, starten Sie den Computer neu, und rufen Sie TCP/IP wieder auf.

Alle oben genannten Programme verwenden Treiber, die mit niedrigeren Ebenen des mit WinRoute ausgeführten Netzwerkprotokolls nicht ordnungsgemäß arbeiten.

Routing-Tabelle

Trotz der ordnungsgemäßen Installation und Konfiguration der Komponenten, können unter Umständen Fehlfunktionen auftreten. Leider ist das Betriebssystem Windows 95/98/NT nicht besonders für die Netzwerke geeignet. Manchmal funktioniert die Einrichtung auch dann nicht, wenn Sie WinRoute installiert haben und die Netzwerkeinstellungen korrekt sind. Sehen Sie in diesem Fall in der Routing-Tabelle nach, und wählen Sie eine der folgenden Möglichkeiten aus:

- Fixieren Sie die Routen, indem Sie sie zunächst löschen und dann wieder hinzufügen - nur für erfahrene Benutzer

oder

- Entfernen Sie das TCP/IP-Protokoll komplett, fahren Sie den Computer erneut hoch, und fügen Sie es wieder hinzu. Die Leistungsfähigkeit ist garantiert.

Proxy Client-Software

Bei manchen PROXY-Servern ist es notwendig, dass auf allen Client-Maschinen Software installiert wird. Auf Grund der Client-Software werden Anfragen von den Anwendungen an den PROXY-Server gesendet. Falls die PROXY-Software des Client nicht entfernt wird, kann dieser Computer nicht mit dem Internet verbunden werden, da WinRoute nicht als PROXY-Server eingerichtet ist. Falls der Client nach wie vor keine Verbindung zum Internet herstellen kann, installieren Sie TCP/IP und die entsprechenden Einstellungen neu, und starten Sie den Computer erneut.

Netzwerkkarten-Treiber

Versuchen Sie die standardisierten Netzwerkkarten zu verwenden. Wenn eine spezielle, alte oder sehr neue Karte in Ihrem Computer installiert ist, verfügt der entsprechende Treiber möglicherweise über spezielle Anweisungen, die die Kommunikation mit WinRoute verhindert. Versuchen Sie, eine standardisierte Ethernet-Karte in Ihrem Netzwerk zu finden und deren Position auszutauschen. Nicht wenige ursprünglich "unzufriedene" Kunden wurden zu "zufriedenen" Kunden, nachdem sie lediglich die Karte ausgetauscht oder den Treiber aktualisiert haben.

WinRoute ist eine völlig neutrale Router/Firewall-Software, bei der es nicht erforderlich ist, Client-Software auf Client-Computern auszuführen. Es sei denn, Sie verwenden die Fernverwaltung. In diesem Fall muss auf dem Client-Computer oder dem externen Computer die "wradmin.exe" für Fernverwaltung installiert werden.

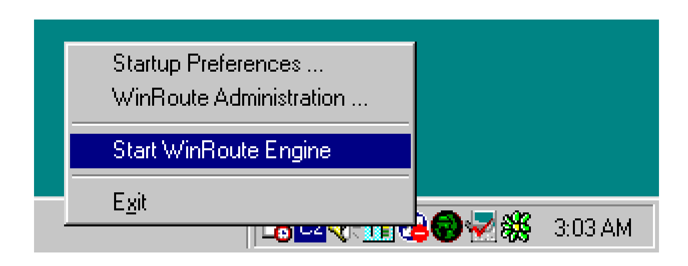
Verwalten mit WinRoute

In diesem Abschnitt

Verwalten des lokalen Netzwerks

Um WinRoute über das lokale Netzwerk oder den WinRoute-Computer zu verwalten, müssen Sie Folgendes ausführen:

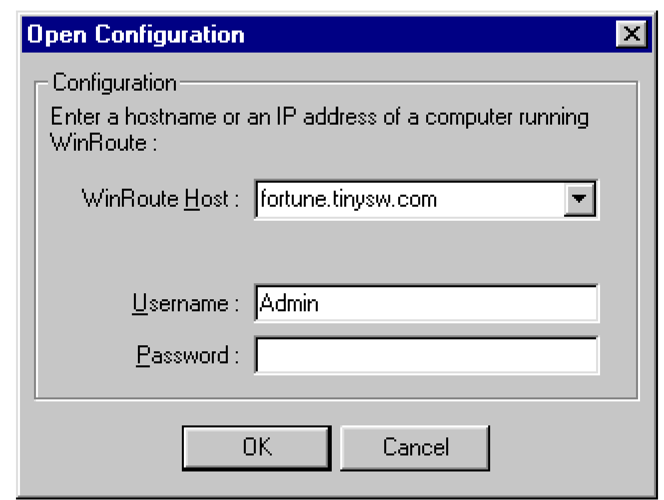
1. **Überprüfen Sie, dass die WinRoute Engine aktiviert ist.**
   Um zu überprüfen, ob WinRoute gestartet wurde, setzen Sie den WinRoute Engine Monitor aus der WinRoute Programmgruppe ein. Ein kleines, rundes blau-weißes Symbol erscheint in der Taskleiste (unten rechts auf dem Desktop). Dies zeigt an, dass die Anwendung aktiv ist. Ist das Symbol mit einem roten Kreuz versehen, bedeutet dies, dass WinRoute gestoppt wurde. Um die WinRoute-Engine zu starten, klicken Sie einfach mit **der rechten Maustaste** auf das Symbol, und wählen Sie in dem daraufhin erscheinenden Menü "WinRoute Engine starten" aus.



2. Starten Sie WinRoute Administrator

Um das WinRoute Administration-Modul zu starten, aktivieren Sie die Anwendung über das Menü Start=>Programme=>WinRoute, oder klicken Sie mit der rechten Maustaste auf das Symbol für den WinRoute Engine Monitor, und wählen Sie *WinRoute Administration* aus dem angezeigten Menü. Sie können auch die *WRAdmin.exe*-Datei auf jedem anderen Computer Ihres Netzwerks kopieren und von dort aus ausführen.

Das Admin-Fenster wird angezeigt. Behalten Sie entweder den voreingestellten lokalen Host-Computer oder geben Sie die IP-Adresse des Computers an, auf dem WinRoute ausgeführt wird. Geben Sie den Benutzernamen sowie das für Administration verwendete Kennwort ein.



Hinweis: Wenn Sie sich zum ersten Mal anmelden, können Sie "Admin" als Benutzernamen verwenden und kein Kennwort eingeben. Weitere Details zur Verfahrensweise im Hinblick auf Benutzernamen und Kennwort für die Verwaltung finden Sie unter Benutzerkonfiguration.

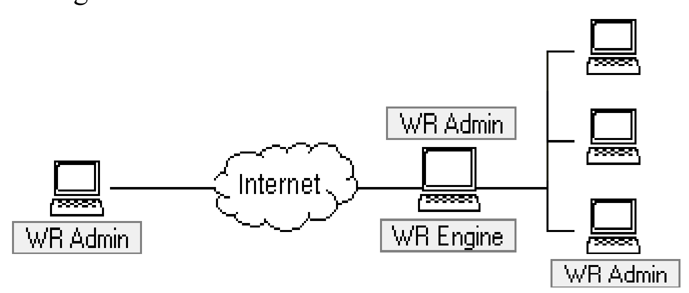
Sie müssen sich als Administrator erfolgreich bei WinRoute Engine anmelden, um Einstellungen vorzunehmen.

Mögliche Gründe für eine fehlgeschlagene Anmeldung über ein lokales Netzwerk:

- WinRoute Engine ist nicht installiert und wird nicht ausgeführt.
- Benutzername und Kennwort sind falsch.
- Es wurde eine falsche IP-Adresse beim Verbindungsaufbau mit der WinRoute Engine eingegeben.
- Sie sind nicht für die Verwaltung von WinRoute berechtigt.
- An der Schnittstelle zu Ihrem Netzwerk ist NAT aktiv (siehe die Kapitel über Checkliste und Netzwerkeinrichtung in dieser Hilfe).

Verwalten über das Internet

Sie können die WinRoute Pro Engine von jedem Computer der Welt aus verwalten, solange Sie vor Ort über eine TCP/IP-Verbindung verfügen. Administration ist sicher (verschlüsselt) und durch den Benutzernamen und das Kennwort geschützt.



Um WinRoute von außerhalb des lokalen Netzwerks zu verwalten, muss die Anschlusszuordnung auf dem Computer installiert sein. Sie müssen berücksichtigen, dass wenn NAT an der Schnittstelle zum Internet auf EIN gestellt ist (dies ist notwendig für den gemeinsamen Internetzugang), Ihr gesamtes Netzwerk einschließlich des WinRoute Computers vollständig geschützt ist, und daher niemand Zugriff auf dieses hat.

Um die Anschlusszuordnung für die Fernverwaltung einzurichten, rufen Sie das Menü *Einstellungen=>Erweitert=>Anschlusszuordnung* auf, klicken Sie auf Hinzufügen und stellen Sie Folgendes ein:

Protokoll: TCP/UDP

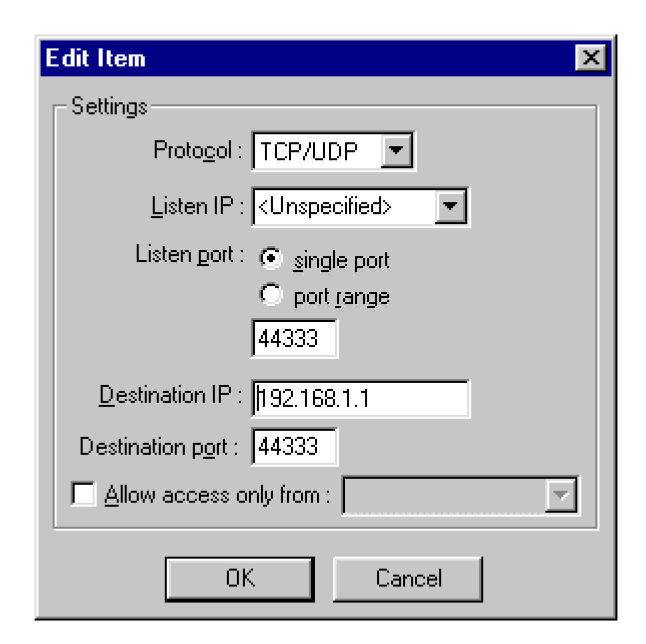
Überwachungs-IP: <nicht spezifiziert> (empfohlen) oder die IP-Adresse der Schnittstelle.

Überwachungsanschluss: 44333

Ziel-IP: Die IP-Adresse der Schnittstelle, die den WinRoute-Computer mit dem lokalen Netzwerk verbindet (private IP-Adresse).

Zielanschluss: 44333

Zugriff nur genehmigen von: Falls aktiviert, können Sie den Zugang zur WinRoute Engine weiter einschränken. Sie müssen IP-Adressen, denen der Zugang zur WinRoute Engine über das Internet erlaubt sein soll, im Menü *Einstellungen=>Erweitert=>Adressengruppen* im Voraus festlegen. Sie können separate IP-Adressen, IP-Adressbereiche und Netzwerke in Gruppen zusammenfassen.



Weitere Einzelheiten über die Anschlusszuordnung können Sie den Beispielen entnehmen. Wenn Sie alles entsprechend eingerichtet haben, führen Sie das Programm WinRoute Administration von einem beliebigen Computer aus, und geben Sie die IP-Adresse des Computers, auf dem WinRoute ausgeführt wird (registriert - z. B. 206.86.181.25) sowie den für Administration festgelegten Benutzernamen und das Kennwort ein. Weitere Details zur Verfahrensweise im Hinblick auf Benutzernamen und Kennwort zur Verwaltung finden Sie unter Benutzerkonfiguration.

Mögliche Gründe für eine nicht erfolgreiche Anmeldung über das Internet:

- WinRoute Engine ist nicht installiert und wird nicht ausgeführt.
- Benutzername und Kennwort sind falsch.
- Es wurde eine falsche IP-Adresse beim Verbindungsaufbau zu WinRoute Engine eingegeben.
- Sie sind nicht berechtigt, WinRoute zu verwalten.

- Die Anschlusszuordnung ist auf dem WinRoute Engine ausführenden Computer nicht oder falsch installiert.

Verlust des Verwaltungskennworts

Falls Sie das Kennwort für Administration verlieren sollten, senden Sie eine E-Mail an support@tinysoftware.com, um weitere Anweisungen zu erhalten. Aus Sicherheitsgründen veröffentlichen wir die entsprechenden Lösungen nicht.

Einrichten des Netzwerks (DHCP)

In diesem Abschnitt

Informationen zu DHCP

Bei Verwendung des DHCP-Servers können Sie die Konfiguration der Workstations innerhalb Ihres lokalen Netzwerks deutlich vereinfachen. Sie müssen die Client-Computer lediglich so einrichten, dass sie vom DHCP-Server dynamisch IP-Adressen zugewiesen bekommen. (Dies ist die Standardeinstellung, wenn das TCP/IP-Protokoll in den Netzwerkeigenschaften hinzugefügt wird.)

Sie können entweder den in WinRoute integrierten DHCP-Server oder den DHCP-Server eines anderen Anbieters innerhalb des Netzwerks verwenden. Vergewissern Sie sich, dass Sie in Ihrem Netzwerk jeweils nur einen DHCP-Server aktiviert haben.

Standard-Gateway im Überblick

WinRoute fungiert als Router. Als solcher macht WinRoute zwei grundlegende TCP/IP-Einstellungen an jedem Computer Ihres Netzwerks erforderlich:

- Weisen Sie eine IP-Adresse zu - entweder manuell oder über den DHCP-Server (z. B. DHCP-Server von WinRoute)
- Richten Sie den Standard-Gateway ein.

Der **Standard-Gateway** an jedem über WinRoute auf das Internet zugreifenden Computer muss der **IP- Adresse** der Ethernet-Schnittstelle des WinRoute-Computers, der die Verbindung zum lokalen Netzwerk herstellt, entsprechen.

Beispiel:

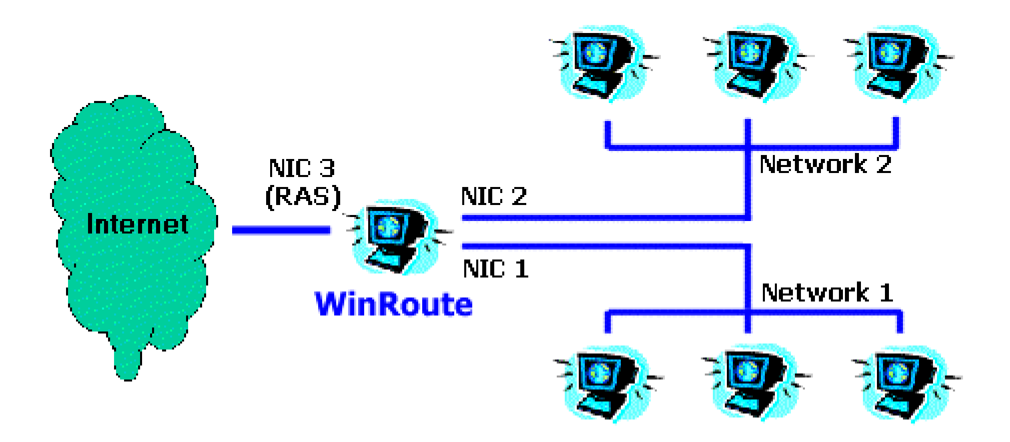
Der Client-Computer hat die IP-Adresse 10.10.10.23, während der WinRoute-PC zwei Schnittstellen hat. Die eine führt zum Kabelmodem mit einer IP von Ihrem Internetdiensteanbieter (z. B. 203.23.14.232), und die andere führt zum privaten Netzwerk (10.10.10.1). Der Standard-Gateway auf dem Computer 10.10.10.23 wird auf 10.10.10.1. eingerichtet.

- ***Hinweis 1: Wenn Sie innerhalb Ihres lokalen Netzwerks Adressplatz für IPs schaffen, müssen Sie die IP-Adressen des gleichen Teilnetzes verwenden. Das heißt, wenn die Maske des verwendeten Teilnetze 255.255.255.0 lautet, müssen sich alle Adressen zwischen 10.10.10.1 und 10.10.10.255. befinden.***
- ***Hinweis 2: Sie können über WInRoute mehrere Netzwerke mit dem Internet verbinden. Innerhalb Ihres WinRoute-Computers können mehrere Schnittstellen vorhanden sein, und zwar eine für jedes Netzwerk. Dann repräsentiert jede dieser Schnittstellen (bzw. ihre IP-Adresse) den Standard-Gateway für den Rest des verbundenen Netzwerks.***

Die Auswahl des geeigneten WinRoute-Computers

WinRoute **MUSS IMMER** auf dem Computer ausgeführt werden, der mit dem Internet über die Netzwerkkarte, Kabel, DSL-Modem, DFÜ-Verbindung oder einen Router verbunden ist.

WinRoute fungiert immer als Gateway zwischen zwei (oder mehreren) Netzwerken, von denen jedes durch eine Schnittstelle repräsentiert wird. Diese Schnittstellen können Ethernet-Karten, RAS-Adapter, USB-nach-Ethernet-Adapter, PPPoE-Adapter usw. sein.

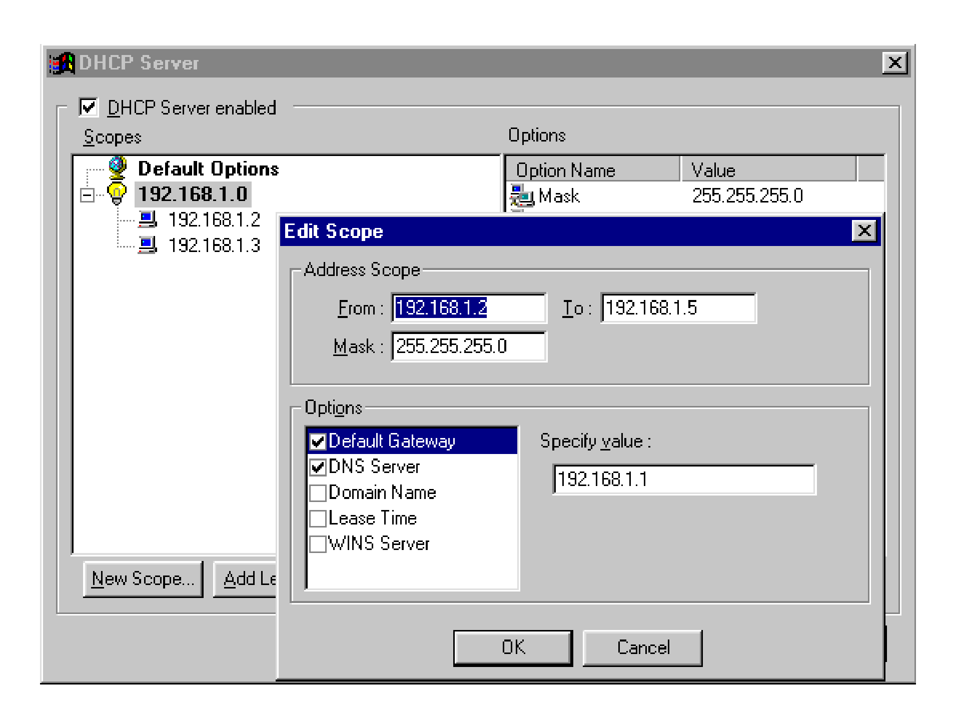

Internet
NIC 3
(RAS)
WinRoute
NIC 2
NIC 1
Network 2
Network 1

IP-Konfiguration mit DHCP-Server

Überprüfen Sie nochmals, dass Ihre Workstations so eingestellt sind, dass sie eine IP-Adresse vom DHCP-Server erhalten (siehe *TCP/IP->Netzwerkschnittstelle-*Eigenschaften bei jedem Computer) und dass alle anderen TCP/IP-Eigenschaften, darunter auch die DNS-Server-Informationen, nicht spezifiziert wurden.

Führen Sie anschließend das WinRoute Administration-Programm aus:

1. Rufen Sie das Menü *Einstellungen=>DHCP-Server* auf.
2. Schalten Sie den DHCP-Server EIN (durch Aktivieren des Kontrollkästchens), und klicken Sie auf die Schaltfläche **Neuer Bereich**.
3. **Neuer Bereich**
   Hier legen Sie den Bereich der vom DHCP-Server verwendeten IP-Adressen fest, die an die Workstations ausgegeben werden. Beachten Sie bitte, dass der WinRoute-Computer bereits eine IP-Adresse verwendet und Sie diese daher nicht verwenden dürfen. Die Bandbreite der IP-Adressen muss der des Teilnetzes entsprechen. (Siehe Abbildung)
4. **Optionen spezifizieren (wichtig!)**
   Unter "Optionen" legen Sie fest, welche anderen Informationen an die Netzwerkcomputer weitergegeben werden (z. B. Standard-Gateway, DNS-Server usw.). Aktivieren Sie die Schaltfläche neben jeder Komponente im Dialogfeld, und geben Sie die entsprechenden Informationen ein. Fügen Sie die Informationen für den Standard-Gateway und den DNS-Server ein (in der Regel wird WinRoute als DNS-Server verwendet), und verwenden Sie die IP-Adresse des WinRoute-Computers (z. B. 192.168.1.1). Die anderen Optionen können Sie freilassen.


DHCP Server
DHCP Server enabled
Scopes
Options
Default Options
192.168.1.0
192.168.1.2
192.168.1.3
Option Name
Value
Mask
255.255.255.0
New Scope...
Add Le
Edit Scope
Address Scope
From :
192.168.1.2
To :
192.168.1.5
Mask :
255.255.255.0
Options
Default Gateway
DNS Server
Domain Name
Lease Time
WINS Server
Specify value :
192.168.1.1
OK
Cancel

- ***Hinweis: Die IP-Adresse der Ethernet-Schnittstelle (Verbindung zum LAN) auf dem WinRoute-Computer muss zugewiesen werden. Diese IP-Adresse wird auf den anderen Computern als Standard-Gateway und in der Regel als DNS-Server eingerichtet!***

IP-Konfiguration mit einem fremden DHCP-Server

Wenn Sie einen DHCP-Server eines anderen Anbieters verwenden, achten Sie insbesondere auf die von einem diesem Server an die Client-Computer innerhalb Ihres Netzwerks ausgegebenen Werte.

Vergewissern Sie sich nochmals, dass Ihr DHCP-Server die richtigen Daten an Ihre Client-Computer weitergibt! Der DHCP-Server muss so eingestellt sein, dass er anderen Computern die IP-Adresse der LAN-Karte des WinRoute-Computers als Standard-Gateway und (optional) als DNS-Server zuweist.

Auch die IP-Adresse, die an die Client-Workstation ausgegeben wird, muss aus dem gleichen Teilnetz stammen wie der WinRoute-Computer.

VERGEWISSERN SIE SICH NOCHMALS, dass der internen Netzwerkkarte des WinRoute-Computers eine feste IP-Adresse (z. B. 192.168.1.1) **zugewiesen ist** und dass diese Adresse vom DHCP als Standard-Gateway an den Rest des Netzwerks weitergegeben wird. Der DHCP-Server darf dem WinRoute-Host keine IP-Adresse zuweisen!

Beispiel:

Der NT-Server mit DHCP wird an 192.168.1.1 ausgeführt, wohingegen WinRoute an 192.168.1.5 ausgeführt wird. Die Daten des Standard-Gateway (und DNS bei Verwendung von WinRoute DNS), die an die Workstations ausgegeben werden, lauten 192.168.1.5.

IP-Konfiguration - manuelle Zuweisung

In einigen Fällen muss man den Workstations IP-Adressen manuell zuweisen. Hierbei sollten Sie folgende Regeln beachten:

IP-Adresse zuweisen

Weisen Sie jedem Computer eine "interne" IP-Adresse zu. Normalerweise 192.168.x.x oder 10.x.x.x. Weisen Sie jedem System IP-Adressen des gleichen Teilnetzes zu. Wenn Sie die IP-Adresse für den WinRoute-Host auf 192.168.1.1 eingestellt haben, müssen Sie mit dem gleichen Nummerierungssystem fortfahren (z. B. 192.168.1.2., 192.168.1.3 usw.).

Standard-Gateway einrichten

Verwenden Sie die IP-Adresse des WinRoute Host-Computers als Standard-Gateway auf allen Client-Computern. Mit anderen Worten heißt das, jeder Client-Computer verwendet die IP-Adresse des WinRoute-Hosts (interne IP-Adresse) als Standard-Gateway. Dies wird am TCP/IP=>Ethernet-Adapter in den Netzwerkeigenschaften des Computers festgelegt.

DNS einrichten

Verwenden Sie die IP-Adresse des WinRoute-Computers für die DNS-Weiterleitung an alle Computer (unter Verwendung des DHCP-Servers von WinRoute die interne IP-Adresse). Die einzige Ausnahme könnte sein, wenn Sie die DNS-Adresse Ihres Internetdiensteanbieters oder eines anderen DNS-Servers verwenden. Geben Sie in diesem Fall die DNS-Angaben ein, die Sie von Ihrem Internetdiensteanbieters erhalten haben (in TCP/IP->NIC Eigenschaften jeder Workstation).

Wichtig! Weitere DNS-Einstellungen finden Sie in dem entsprechenden Kapitel dieses Handbuchs.

Einrichten des DNS-Forwarder

Der DNS-Server wird über das Menü *Einstellungen => DNS -Server* konfiguriert.

"DNS-Weiterleitung aktivieren"

Diese Option überprüft, ob der DNS-Server ein- oder ausgeschaltet ist.

"DNS-Abfragen an den Server weiterleiten, der automatisch von den dem Betriebssystem bekannten DNS-Servern ausgewählt wird."

Falls aktiviert, werden alle DNS-Abfragen an den DNS-Server weitergeleitet, der von der TCP/IP-Konfiguration der Internetschnittstelle oder der DFÜ-Verbindung ausgewählt wurde.

"Suche in HOST-Datei aktivieren"

Wenn diese Option aktiviert ist, ist es dem DNS-Server erlaubt, Daten der HOST-Datei zu verwenden, um die Abfragen zu beantworten.

"HOSTS-Datei bearbeiten..."

Diese Schaltfläche startet einen externen Text-Editor, mit dem Sie die HOSTS-Datei bearbeiten können.

"DNS-Domäne"

Geben Sie hier Ihren Domänennamen ein (z. B. "acme.com"). Wird eine DNS-Abfrage beantwortet, wird der Domänenname an den von der HOSTS-Datei oder von der DHCP Lease-Tabelle erhaltenen Namen angehängt.

"DNS-Abfragen weiterleiten an"

Geben Sie die numerische IP-Adresse des DNS-Servers ein, an den die DNS-Abfragen weitergeleitet werden sollen. Wählen Sie eine Adresse des DNS-Servers Ihres Internetdiensteanbieters oder eines Servers, zu dem Sie schnellen Zugang besitzen.

"DNS-Cache aktivieren"

Mit dieser Option können Antworten auf DNS-Abfragen im internen Cache gespeichert werden. Nachfolgende Abfragen werden dann bearbeitet, indem der Inhalt des Cache verwendet wird, ohne auf eine Antwort des DNS-Servers außerhalb Ihres Netzwerks zu warten.

"Beim Auflösen des Namens aus der HOSTS-Datei oder der Lease-Tabelle diesen mit der DNS-Domäne verbinden"

Diese Funktion lässt sich besser anhand eines Beispiels erklären. Nehmen wir an, Sie möchten eine Antwort auf eine DNS-Abfrage für den Computer MEIER finden. In der HOSTS-Datei haben Sie eingegeben, dass Ihre Domäne BÜRO mit einer speziellen IP-Adresse assoziiert ist. Dann könnte die Abfrage MEIER.BÜRO richtig beantwortet werden.

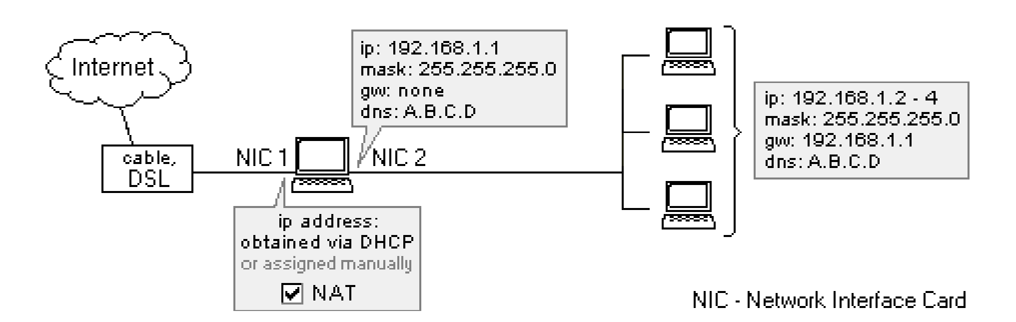
➢ ***Beachten Sie bitte, dass der Cache nur Antworten des Typs "Name => IP-Adresse" speichert. Die Antworten werden solange gespeichert, bis sie ungültig werden. Die Gültigkeitsdauer wird vom DNS-Server zusammen mit der Antwort geliefert.***

Herstellen der Internetverbindung

In diesem Abschnitt

DSL-Verbindung

Für die DSL- (ADSL-, SDSL-)Verbindung müssen zwei Netzwerkkarten (NICs) auf dem WinRoute-Computer installiert sein. Eine Netzwerkkarte führt zum Internet (DSL -Modem), die andere zum internen Netzwerk.



WinRoute-Konfiguration

Führen Sie folgende Schritte aus, um eine Verbindung zum Internet herzustellen:

1. Gehen Sie zum Menü Einstellungen -> Schnittstellentabelle.
2. Wählen Sie die Netzwerkkarte, die zum Internet führt aus, klicken Sie auf "Eigenschaften", und aktivieren Sie "NAT mit der IP-Adresse dieser Schnittstelle für den gesamten, passierenden Datenverkehr ausführen". Wenn Sie das Dialogfeld "Schnittstellentabelle" öffnen, sehen Sie neben dieser externen Verbindung NAT EIN angezeigt.
3. Überprüfen Sie, dass NAT an der Schnittstelle zum internen Netzwerk NICHT EIN ist. (Gehen Sie zu den Eigenschaften dieser Schnittstelle in der Schnittstellentabelle.)
4. Überprüfen Sie, dass KEIN Gateway in den TCP/IP-Eigenschaften der internen Netzwerkkarte eingerichtet ist. (Gehen Sie zu den Netzwerkeinstellungen.) Vergewissern Sie sich außerdem, dass der Netzwerkkarte eine IP-Adresse zugewiesen ist.
5. Überprüfen Sie, dass die Netzwerkkarte zum Internet mit den Daten von Ihrem Internetdiensteanbieters richtig zugewiesen wurde. Falls Sie dynamisch zugewiesene IP-Adressen haben, lassen Sie die IP-Adresseinstellungen frei.

Weitere Netzwerkeinstellungen finden Sie in den entsprechenden Kapiteln, insbesondere unter ***Checkliste*** .

PPPoE-DSL-Verbindung

PPPoE ist eine vor kurzem eingesetzte Technik für viele DSL-Abonnenten bzw. -Teilnehmer. Wenngleich es derzeit von verschiedenen Internetdiensteanbietern umfassend eingesetzt wird, bietet es den Benutzern unzureichende Leistung und ist (derzeit) nicht die bestmögliche Lösung für die Anbindung Ihres Netzwerks an das Internet. Der Kunde sollte, wenn möglich, die Standard-DSL-Lösung verwenden.

Im Hinblick auf die TCP/IP-Einstellungen ist der Einsatz von PPPoE mit WinRoute mit der Standard-DSL vergleichbar. WinRoute Pro sollte auf dem gleichen Computer installiert werden wie der PPPoE-Adapter. Das Programm erkennt den PPPoE-Adapter als Netzwerkschnittstelle. An dieser Schnittstelle sollten Sie NAT aktivieren. Der Ethernet-Adapter (an das Kabelmodem angeschlossen) erscheint in der Schnittstellentabelle von WinRoute Pro als Schnittstelle. An dieser Schnittstelle sollten Sie NAT nicht aktivieren.

WinRoute Pro ist mit allen auf dem Markt erhältlichen PPPoE-Adaptern zusammen. Manchmal können Kunden jedoch bei bestimmten PPPoE-Adaptern verschiedene Leistungseigenschaften feststellen:

Enternet 100, 300, 500 PPPoE-Client

WinRoute Pro 4.1 funktioniert mit dem Enternet PPPoE-Client von NTS gut, wenn Sie statt des Standard-Filter-Treibers den Protokoll-Treiber aktivieren. Führen Sie hierzu den Ethernet PPPoE-Client aus, rufen Sie das Menü Einstellungen -> Erweitert auf, und ändern Sie die gewünschten Werte.

Wenn Sie Schwierigkeiten bezüglich der Leistungsfähigkeit feststellen, reduzieren Sie den Wert für MTU auf den Client-Computern auf 800.

WinPoet von Ivasion

WinRoute Pro 4.1 ist unter folgenden Bedingungen mit WinPoet kompatibel: IP-Header-Kompression (RAS/Einwähl-Netzwerkeinstellungen) ist ausgeschaltet.

Verringern des MTU-Wertes:

Der PPPoE-Adapter fügt ergänzende Informationen zum Header jedes ausgehenden Pakets hinzu. Windows verwendet standardmäßig die maximal erlaubte Paketgröße. Der PPPoE-Adapter kompensiert dies dadurch, dass er garantiert, dass der MTU-Wert des lokalen Computers leicht verringert wird, um die zusätzlichen zu jedem Paket hinzugefügten Informationen auszugleichen. Leider verwenden alle anderen Computer immer noch die maximale Größe für die Übertragung. Dies führt zum Verlust von Paketen. Die folgenden Links zeigen Ihnen, wie der MTU-Wert an allen Clients verringert wird.

Für Benutzer von Windows 95/98 :

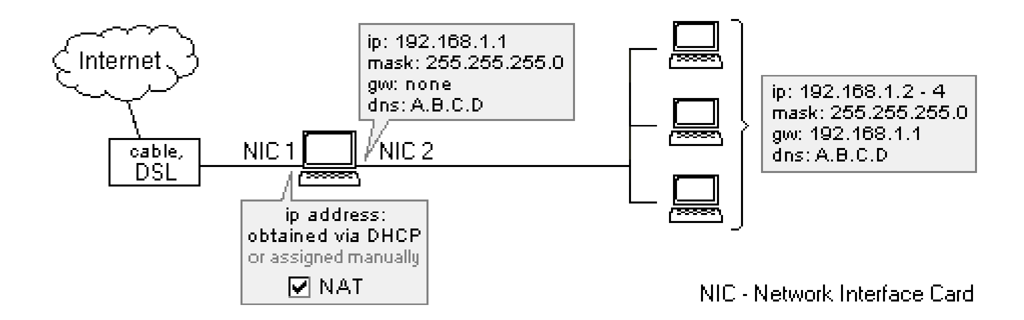
http://www.microsoft.com/support/kb/articles/Q158/4/74.asp

Für Benutzer von Windows NT4/2000 :

http://www.microsoft.com/WINDOWS2000/library/resources/reskit/samplechapters/cnbd/cnbd_trb_vcfx.asp

Bidirektionale Kabelmodemverbindung

Für die Verbindung durch Kabelmodem sind zwei Netzwerkkarten (NIC) im WinRoute-Computer notwendig. Eine Netzwerkkarte führt zum Internet (Kabelmodem), die andere NIC zum internen Netzwerk. Weitere Informationen bezüglich eines unidirektionalen Kabelmodems (Modem in Betrieb, Kabel außer Betrieb) finden Sie in den entsprechenden Kapiteln.



WinRoute-Konfiguration

1 Rufen Sie das Menü Einstellungen->Schnittstellentabelle auf.

2 Wählen Sie die Netzwerkkarte aus, die zum Internet führt, klicken Sie auf Eigenschaften, und aktivieren Sie " NAT ausführen mit der IP-Adresse der Schnittstelle für die gesamte das Netz passierende Kommunikation". Wenn Sie das Dialogfeld Schnittstellentabelle öffnen, wird neben dieser externen Leitung NAT EIN angezeigt.

3 Überprüfen Sie, dass für NAT an der Schnittstelle zum internen Netzwerk NICHT EIN angezeigt ist. (Rufen Sie die Eigenschaften dieser Schnittstelle in der Schnittstellentabelle auf.)

4 Überprüfen Sie, dass KEIN Gateway in den TCP/IP-Eigenschaften der internen Netzwerkkarte eingerichtet ist (rufen Sie die Netzwerkeinstellungen auf) und der Netzwerkkarte eine interne IP-Adresse zugewiesen wurde.

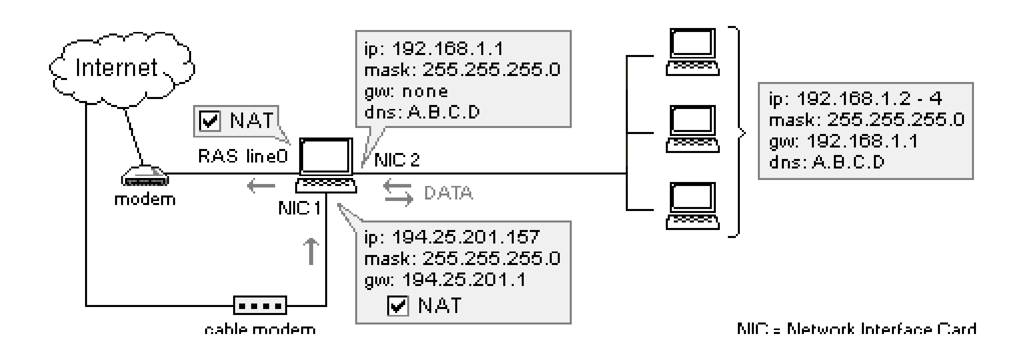
5 Überprüfen Sie, dass der zum Internet führenden Netzwerkkarte die Daten Ihres Internetdiensteanbieters zugewiesen wurden. Bei dynamisch zugewiesenen IP-Adressen geben Sie keine IP-Adressen-Einstellungen ein.

Weitere Netzwerkeinstellungen finden Sie in den entsprechenden Kapiteln (z. B. ***Checkliste*** , ***IP-Konfiguration***)

Unidirektionales Kabelmodem (Modem in Betrieb, Kabel ausser Betrieb)

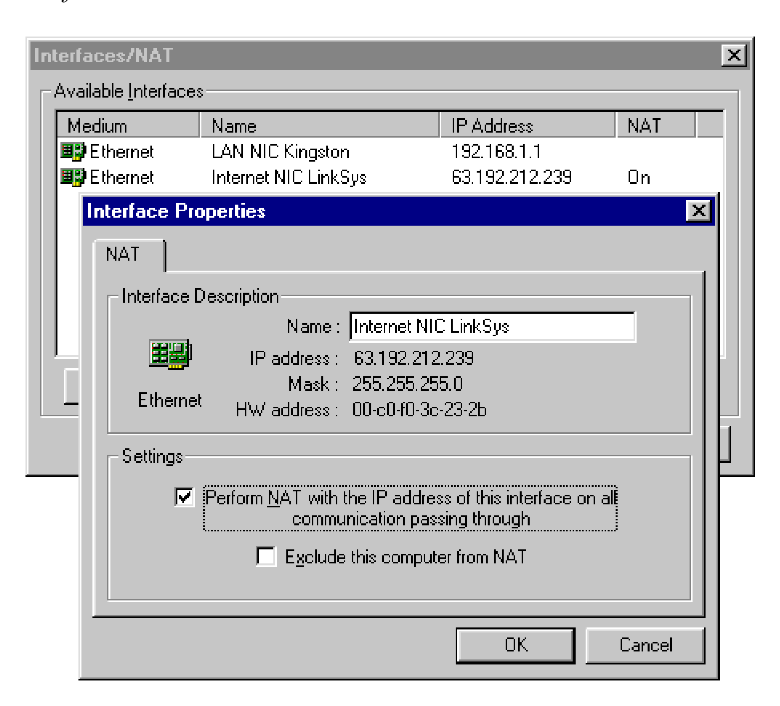
HINWEIS: Diese Art der Internetverbindung ist **"keine offiziell unterstützte Konfiguration",** da die Einstellungen von Anbieter zu Anbieter **variieren können**. Wir versuchen jedoch, Zugangslösungen für möglichst viele verschiedene Umgebungen zu bieten. Für die meisten unserer Benutzer war der Verbindungsaufbau mit folgenden Einstellungen erfolgreich.

Im Allgemeinen ähnelt der Datenverkehr dem **von DirecPC**. Ausgehende Pakete passieren die **DFÜ-Schnittstelle.** Auf dem Rückweg werden sie **über ein Kabel** geleitet. Im Grunde muss Ihr Internetdiensteanbieter Ihre beiden Schnittstellen einander zuordnen. Dies erscheint schwierig, ist aber der einzige Weg, um eine funktionsfähige Verbindung aufzubauen. Daher empfehlen wir Ihnen, Rücksprache mit Ihrem ISP zu halten, bevor Sie WinRoute erwerben.



1. Rufen Sie das Menü *Einstellungen->Schnittstellentabelle* auf. Hier werden eine Schnittstelle der **RAS-Leitung** (Ihr Modem) und zwei **Netzkartenschnittstellen** angezeigt - eine für die Verbindung mit dem Internet, die andere für die Verbindung mit dem lokalen Netzwerk.

2. Klicken Sie auf die zum Internet führende Netzwerkkarte, und rufen Sie das Menü *"Eigenschaften"* auf. Aktivieren Sie das Kontrollkästchen *"NAT mit der IP-Adresse dieser Schnittstelle für den gesamten, passierenden Datenverkehr ausführen"*.



3. Klicken Sie auf **RAS-Schnittstelle**, und rufen Sie *"Eigenschaften"* auf. Aktivieren Sie das Kontrollkästchen "*NAT mit der IP-Adresse dieser Schnittstelle für den gesamten, passierenden Datenverkehr ausführen"*. Wählen Sie auf der **Registerkarte RAS** die Verbindung aus für den Verbindungsaufbau zu Ihrem ISP aus. Geben Sie anschließend Ihren Benutzernamen und das Kennwort ein.

4.Vergewissern Sie sich, das NAT an der Schnittstelle zum internen Netzwerk **NICHT EIN** ist (wechseln Sie zu den Eigenschaften dieser Schnittstelle).

5. Überprüfen Sie, dass in den TCP/IP -Eigenschaften der internen Netzwerkkarte **KEIN Gateway** eingerichtet ist (wechseln Sie zu den Netzwerkeinstellungen) und dass der Netzwerkkarte eine private **IP-Adresse** zugewiesen ist (z. B. 10.10.1.1).

6. Überprüfen Sie, dass der zum Internet führenden Netzwerkkarte die Daten Ihres ISP (TCP/IP-Eigenschaften) zugewiesen wurden. Hinweis: Bei dynamisch zugewiesenen IP-Adressen lassen Sie die IP-Adresseinstellungen frei.

- ***In der Regel sollte NAT an beiden Schnittstellen zum Internet - RAS und DFÜ - auf "EIN" eingestellt sein.***

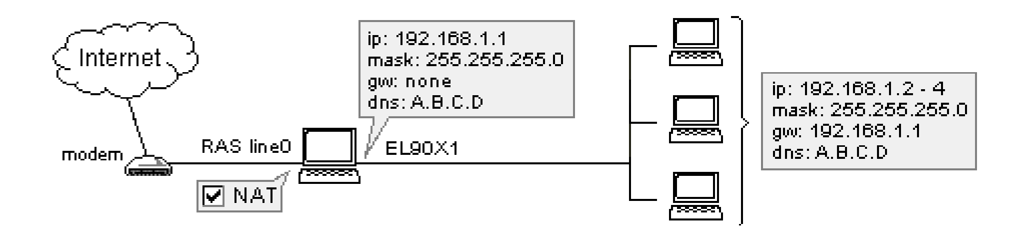
Verbindung über DFÜ oder ISDN

Verbindung über DFÜ oder ISDN

Wenn Sie an einem PC, auf dem Win95, Win98 oder NT4.0 ausgeführt wird, über einen DFÜ-Zugang zum Internet verfügen (die üblichen 56 K oder ISDN), haben Sie alles, was Sie für die Ausführung von WinRoute benötigen. WinRoute muss auf einem Computer ausgeführt werden, auf dem Folgendes installiert ist:

- ein an die Telefon- oder die ISDN-Leitung angeschlossenes Modem

- eine zum internen Netzwerk führende Netzwerkkarte (NIC)



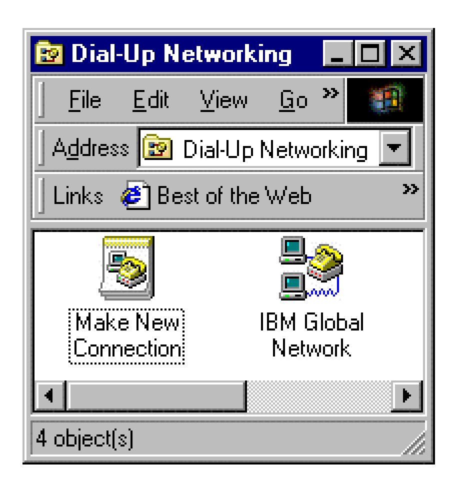
Wenn Sie über ein ISDN-Modem verfügen, das über Ethernet-Karte mit Ihrem Computer verbunden ist, lesen Sie im Kapitel über die Verbindung mit DSL nach. In diesem Fall konfigurieren Sie WinRoute so, dass es mit zwei Ethernet-Karten arbeitet.

Vor dem Verbindungsaufbau

Bevor Sie die Verbindung zum Internet herstellen, überprüfen Sie folgende Punkte:

- Das TCP/IP-Protokoll ist richtig installiert und konfiguriert (siehe Checkliste oder Kapitel zu der Netzwerkeinstellung).
- Das DFÜ-Netzwerk (Windows 95/98) oder der RAS-Dienst (WindowsNT) ist richtig installiert und konfiguriert.
- Das Modem ist an den Host-PC von WinRoute angeschlossen.

Für die Internetverbindung verwendet WinRoute das DFÜ-Netzwerk oder RAS-Dienste, die in Ihrem Betriebssystem zur Verfügung stehen.



Wir empfehlen Ihnen, die Verbindung zwischen dem Internet und dem Computer, auf dem WinRoute installiert werden soll, herstellen, BEVOR WinRoute installiert und ausgeführt wird. Auf diese Weise wird gewährleistet, dass die Verbindung richtig konfiguriert ist und das DFÜ-Netzwerk oder der RAS-Dienst richtig funktioniert.

WinRoute-Konfiguration

Führen Sie folgende Schritte aus, nachdem Sie die gesamte, oben aufgeführte Konfiguration vorgenommen haben:

1. Rufen Sie das Menü Einstellungen->Schnittstellentabelle auf. Hier sollten alle in Ihrem Computer verfügbaren Schnittstellen angezeigt werden. DFÜ-Schnittstellen werden in WinRoute-Betriebssystemen (sowohl in 95/98 und NT) als RAS bezeichnet.
2. Wechseln Sie zu den Eigenschaften der ausgewählten RAS-Schnittstelle.
3. Aktivieren Sie die Schaltfläche "NAT mit der IP-Adresse dieser Schnittstelle für den gesamten, passierenden Datenverkehr".

4 Gehen Sie zur RAS-Tabelle im Dialogfeld Eigenschaften, wählen Sie oder erstellen Sie eine Verbindung, und legen Sie die Optionen entsprechend Ihrer Bedürfnisse fest. Weitere Einzelheiten entnehmen Sie bitte der RAS-Tabelle.

➢ ***Denken Sie daran! NAT muss an der RAS-Schnittstelle "AKTIVIERT" sein, während es an den Schnittstellen zum internen Netzwerk "DEAKTIVIERT" sein muss.***

Ethernet-Schnittstellen-Konfiguration

1 Der Netzwerkkarte zum internen Netzwerk wurde eine (private) IP-Adresse zugewiesen und KEIN Gateway!

2 Die für diese Schnittstelle verwendeten DNS-Einträge basieren auf Daten Ihres Internetdiensteanbieters. Falls Ihnen diese Daten nicht zur Verfügung gestellt wurden, wenden Sie sich bitte an den Diensteanbieter.

Sie können WinRoute zur Verwendung der Wahlaufforderung (Dial-On-Demand) einrichten. Dabei wird die Verbindung automatisch basierend auf dem Datenverkehr, der das lokale Netzwerk verlässt, hergestellt. Wenn Sie Einzelheiten dazu erfahren möchten, klicken Sie hier.

AOL-Verbindung

Wenn Sie WinRoute Pro verwenden, können Sie Ihr Netzwerk über ein einfaches AOL-DFÜ-Konto mit dem Internet verbinden. Hinweis: AOL unterstützt nur Computer mit Win95/98. Um eine Verbindung über AOL herzustellen, führen Sie folgende Schritte aus:

1 Installieren Sie die AOL-Client-Software (vorzugsweise AOL 5.0 oder höher).

2 Stellen Sie eine Internetverbindung her, um zu überprüfen, dass die Verbindung ordnungsgemäß funktioniert.

3 Installieren Sie WinRoute Pro.

4 Rufen Sie in WinRoute Administration das Menü *Einstellungen->Schnittstellentabelle* auf.

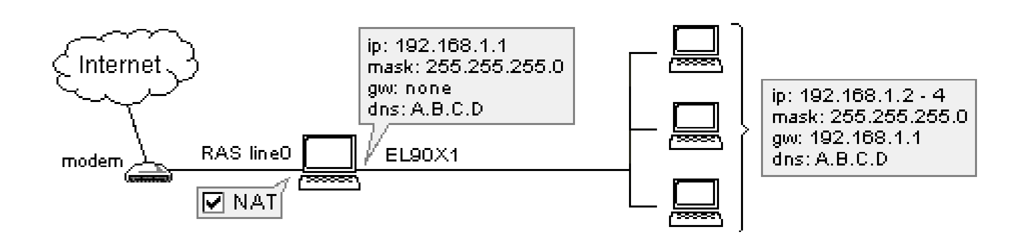
5 Der AOL-Adapter sollte unter den verfügbaren Schnittstellen aufgeführt sein. Klicken Sie auf Eigenschaften einer solchen Schnittstelle, und wählen Sie für diese Schnittstelle "NAT ausführen".

Richten Sie Ihren WinRoute-Computer und die Client-Computer gemäß der Checkliste ein (siehe Kapitel zur Checkliste).

➢ ***Hinweis! Die Wahlaufforderung (Dial-On-Demand) funktioniert in diesem Fall nicht. Sie müssen die Verbindung zu AOL manuell herstellen.***

T1- oder LAN-Verbindung

Für T1- oder LAN-Verbindungen müssen zwei Netzwerkkarten auf dem WinRoute-Computer installiert sein. Eine Netzwerkkarte führt zum Internet (z. B. Router), die andere zum internen Netzwerk.



Führen Sie folgende Schritte aus, um die Verbindung zum Internet herzustellen:

1 Rufen Sie das Menü Einstellungen->Schnittstellentabelle auf.

2 Wählen Sie die Netzwerkkarte, die zum Internet führt, klicken Sie auf Eigenschaften, und aktivieren Sie "NAT mit der IP-Adresse dieser Schnittstelle für den gesamten, passierenden Datenverkehr ausführen". Wenn Sie auf die Schaltfläche Schnittstellentabelle klicken, wird neben der externen Verbindung NAT EIN angezeigt.

3 Überprüfen Sie, dass NAT für die Schnittstelle zum internen Netzwerk NICHT EIN ist. (Rufen Sie die Eigenschaften dieser Schnittstelle in der Schnittstellentabelle auf.)

4 Vergewissern Sie sich, dass in den TCP/IP-Eigenschaften der internen Netzwerkkarte KEIN Gateway eingerichtet ist (wechseln Sie zu den Netzwerkeinstellungen) und dass der Netzwerkkarte eine interne IP-Adresse zugewiesen wurde.

5 Überprüfen Sie, dass der zum Internet führenden Netzwerkkarte die Daten Ihres Internetdiensteanbieters ordnungsgemäß zugewiesen wurden. Bei einer dynamisch zugewiesenen IP-Adresse lassen Sie die IP-Adresseinstellungen frei.

Weitere Netzwerkeinstellungen finden Sie in den entsprechenden Kapiteln, insbesondere im Kapitel ***Checkliste*** .

DirecPC-Verbindung

DirecPC verwendet ein Modem (analog, ISDN usw.) oder eine Netzwerkkarte (Ethernet, Token Ring) für die Aufwärtsverbindung, während zum Herunterladen der Daten eine Satellitenschüssel eingesetzt wird. Ihre Internetverbindung wird von DirecPC selbst bereitgestellt. Alternativ können Sie auch den vorhandenen Dienst Ihres Internetdiensteanbieters für die DFÜ-Verbindung verwenden.

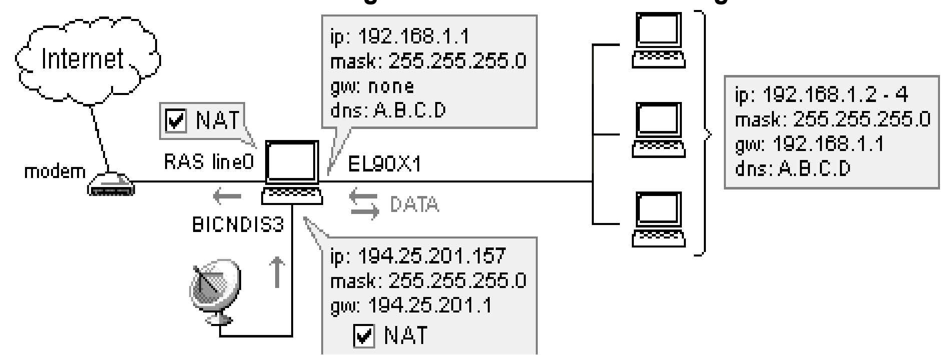
Die Daten werden von Ihrem Computer über das Modem zum DirecPC-Internetdienst übertragen, wo sie zu ihrem endgültigen Bestimmungsort geleitet werden. Auf dem Rückweg verknüpft DirecPC die Pakete (Daten), die an Ihrem Computer ankommen, mit verschiedenen Daten, um sie über die Satellitenschüssel zu leiten.

WinRoute-Konfiguration

Zunächst müssen Sie die gesamte DirecPC-Software und die Komponenten ordnungsgemäß installieren. Anschließend können Sie WinRoute Ihren speziellen Bedürfnissen entsprechend konfigurieren.

Für die Aufwärtsverbindung können Sie entweder die DirecPC-Wahlhilfe oder WinRoute-RAS verwenden. Mit WinRoute können Sie von der Wahllaufforderungsfunktion (Dial-On-Demand) profitieren, die Ihnen eine erhebliche Kostenersparnis einbringt.

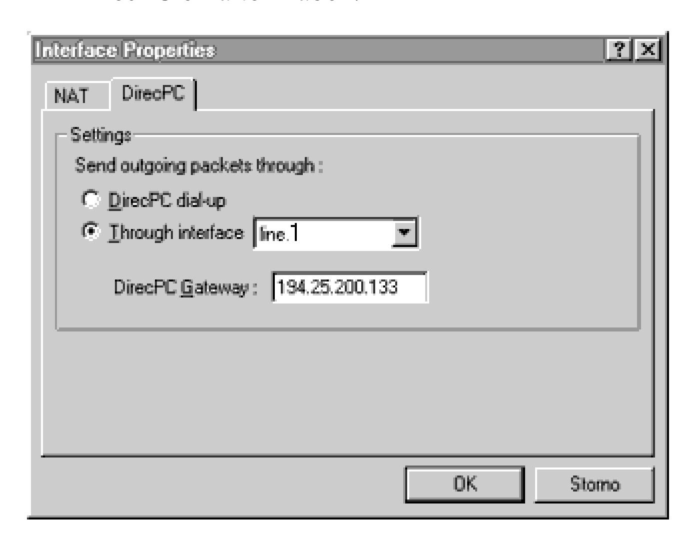
1. Verwenden der RAS-Leitung für die Aufwärtsverbindung



Rufen Sie das Menü *Einstellungen->Schnittstellentabelle* auf. Hier wird die Schnittstelle der RAS-Leitung (Ihr Modem) und die DirecPC-Netzwerkkarte angezeigt.

Klicken Sie auf die DirecPC-Netzwerkkarte und anschließend auf "Eigenschaften". Es werden zwei Registerkarten angezeigt: **NAT** und **DirecPC**.

- Aktivieren Sie auf der Registerkarte "NAT" das Kontrollkästchen *"NAT mit dieser Schnittstelle für den gesamten, passierenden Datenverkehr ausführen"*.
- Wählen Sie auf der Registerkarte "DirecPC" *line0* für die Aufwärtsverbindung. Geben Sie die G*ateway-IP-Adresse* ein, die Sie von DirecPC erhalten haben.

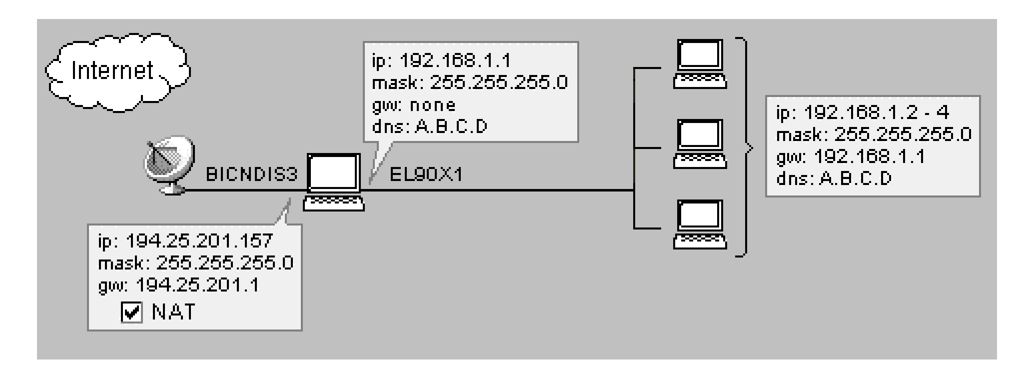


3. Klicken Sie auf die RAS-Schnittstelle und anschließend auf "Eigenschaften". Aktivieren Sie " NAT mit der IP-Adresse dieser Schnittstelle für den gesamten, passierenden Datenverkehr ausführen". Wählen Sie auf der Registerkarte "RAS" die Verbindung zu Ihrem Internetdiensteanbieters aus. Geben Sie anschließend Ihren Benutzernamen und das Kennwort ein.

➢ ***Hinweis! Deaktivieren Sie das Kontrollkästchen "Standard-Gateway am Fernnetz verwenden" in den Eigenschaften des DFÜ-Netzwerkkontos, das erstellt wird, um die Verbindung mit dem Internetdiensteanbieters herzustellen. Richten Sie diese Option in den TCP/IP-Eigenschaften Ihrer DFÜ-Schnittstelle ein.***

2. Verwenden der DirecPC-Wahlhilfe für den Verbindungsaufbau

Sie können, falls verfügbar, die in DirecPC integrierte Wahlhilfe verwenden. Wir empfehlen jedoch, wenn möglich, die WinRoute RAS-Leitung zu verwenden.



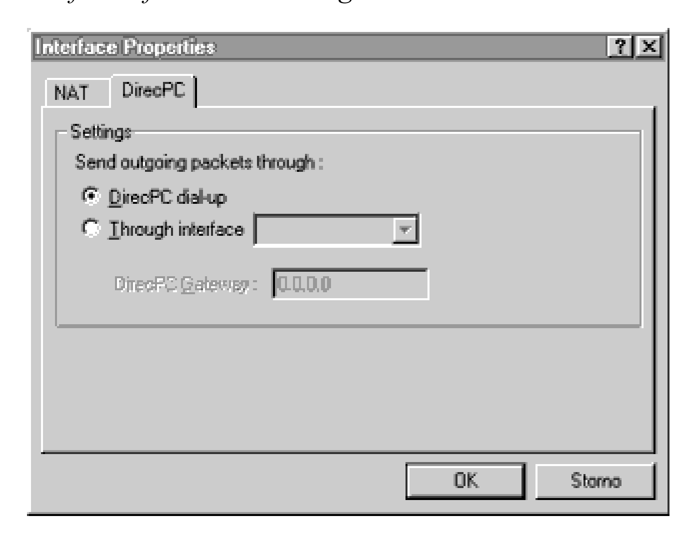
So verwenden Sie die DirecPC-Wahlhilfe:

Rufen Sie das Menü *Einstellungen->Schnittstellentabelle* auf. Es werden die Schnittstelle der RAS-Leitung (Ihr Modem) und die Netzwerkkarte von DirecPC angezeigt.

Klicken Sie auf die Netzwerkkarte von DirecPC, und wählen Sie "*Eigenschaften*". Es werden zwei Registerkarten angezeigt: NAT und DirecPC.

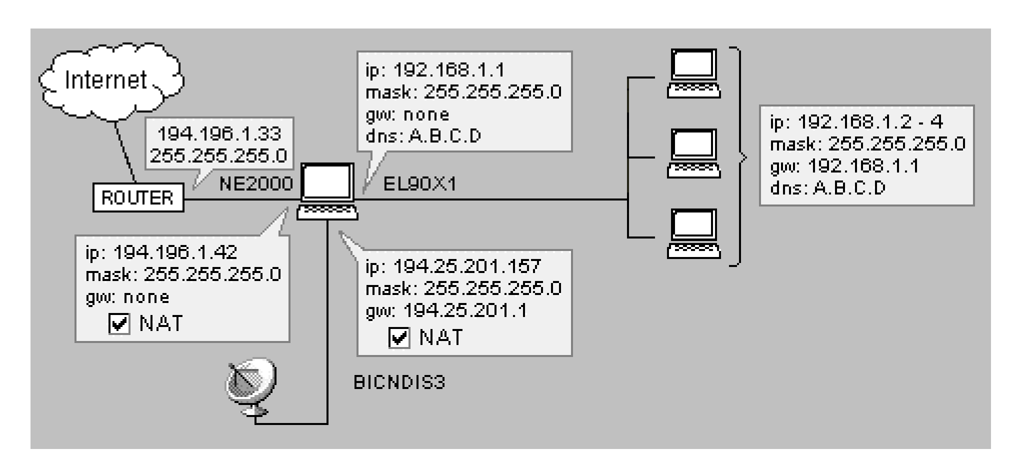
- Aktivieren Sie das Kontrollkästchen "*NAT mit dieser IP-Adresse der Schnittstelle für den gesamten, passierenden Datenverkehr ausführen*" auf der Registerkarte "NAT".

- Wählen Sie auf der Registerkarte "DirecPC" die Option "*DirecPC-Wählhilfe für Aufwärtsverbindung verwenden*".

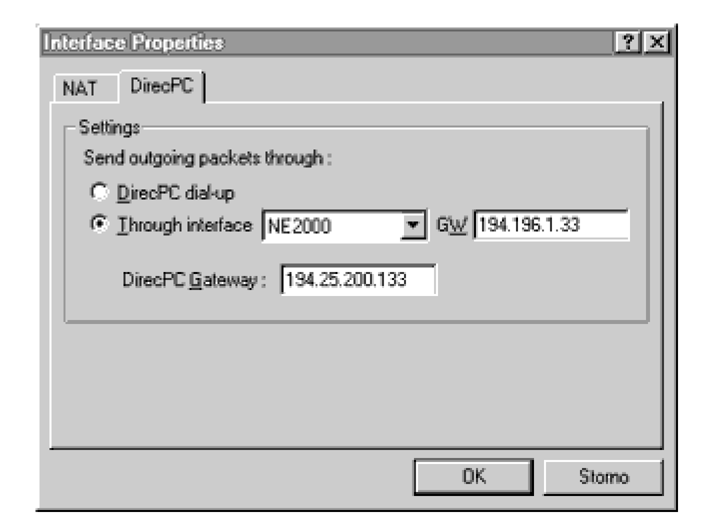


3. Verwenden der Ethernet-Schnittstelle für die Aufwärtsverbindung:

Unter Umständen möchten Sie die Ethernet-Schnittstelle für die Aufwärtsverbindung verwenden. Dies ist in der Regel der Fall, wenn die Aufwärtsverbindung über eine ISDN-Leitung (und Sie über einen ISDN-Router oder ein Modem verfügen) oder über eine V-SAT-Verbindung (Schüssel mit Ethernet-Adapter) erfolgt.



Rufen Sie das Dialogfeld der Eigenschaften der DirecPC-Netzwerkkarte auf.



- Aktivieren Sie auf der Registerkarte "NAT" das Kontrollkästchen "*NAT mit dieser IP-Adresse der Schnittstelle für den gesamten, passierenden Datenverkehr ausführen*".
- Wählen Sie auf der Registerkarte "DirecPC" die Option "*Über Schnittstelle*" und wählen Sie die Schnittstelle zum Internet. Geben Sie dann den Standard-Gateway Ihres Internetdiensteanbieters in das Feld "GW' ein (z. B. 194.196.1.33).

Erhöhen des Datendurchsatzes

Um bei der Verbindung mit dem Internet über DirecPC den größtmöglichen Datendurchsatz zu erhalten, verkleinern Sie das **TCP-Empfangsfenster** auf allen Computern, die DirecPC verwenden:

Unter Windows NT:

1. Rufen Sie die Registrierung HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters auf.
2. Fügen Sie einen Eintrag mit Namen "TcpWindowSize" zur Registrierung hinzu. (Falls er bereits vorhanden ist, bearbeiten Sie diesen.) Stellen Sie seinen Wert auf "0xBB80" ein.

Unter Windows 95:

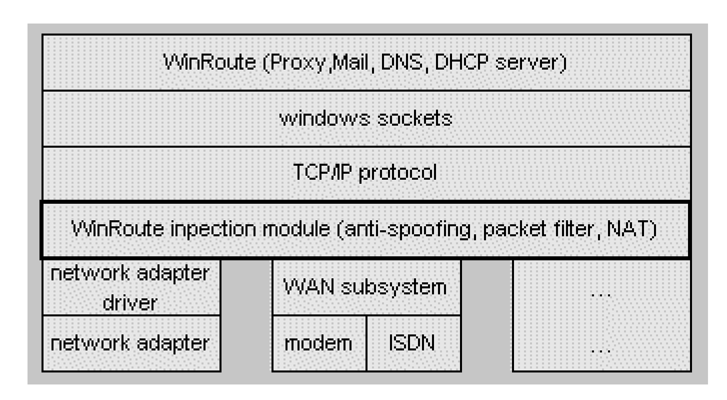
1. Rufen Sie die Registrierung HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP auf.
2. Fügen Sie einen Eintrag mit Namen "DefaultRcvWindow" zur Registrierung hinzu. (Falls er bereits vorhanden ist, bearbeiten Sie diesen.) Stellen Sie seinen Wert auf "0xBB80" ein.

Sicherheitseinstellungen

In diesem Abschnitt

NAT-Sicherheit

WinRoute führt NAT auf der niedrigsten Netzwerk-Protokollschicht aus. Das Programm überprüft den Datenverkehr zwischen dem Treiber der Netzwerkkarte und dem TCP-Stack (Datenstapel). Es kontrolliert den Internetdatenverkehr vollständig, indem es sowohl ausgehende als auch eingehende Pakete erfasst. Somit ist maximale Sicherheit gewährleistet. Diese Funktion zeichnet die NAT-Implementierung von WinRoute aus. WinRoute bietet außerdem zusätzliche Sicherheitsfunktionen, wie eine auf Paketfilter basierende Firewall und Anti-Spoofing. Mit NAT von WinRoute ist das gesamte Netzwerk einschließlich des Computers, auf dem WinRoute ausgeführt wird, geschützt.



NAT- Sicherheitsoptionen

In den erweiterten Einstellungen von WinRoute Build 20 und höher befindet sich ein Menü mit NAT-Sicherheitsoptionen, das einen **Automatikmodus** beinhaltet. **Automatikmodus** bedeutet, dass WinRoute für bestimmte Arten von Anfragen, Pakete "abwerfen" kann, so dass Ihr Netzwerk nach außen unsichtbar erscheint.

Eingehende ICMP Echo-Anfragen:

Internet Control Message Protocol (ICMP) ist das Protokoll, mit dem man einfach eine Informationsanfrage senden kann ("pinging", Beispiel - ping 206.86.211.32). Wenn ein Computer versucht, den WinRoute-Host zu **"pingen",** bieten die **NAT-Sicherheitsoptionen** zwei mögliche Reaktionen:

- Wenn Sie *" ICMP-Echoantwort senden"* wählen, erhält der anfragende Computer eine Antwort.
- Wenn Sie *"Anfrage verwerfen (automatische Installation)"* wählen, wird das Datagramm abgeworfen, d. h., es geht während der Übertragung verloren. Die anfragende Partei erhält dann die Nachricht, dass der Ziel-Host nicht erreichbar ist.

Eingehende Pakete ohne Eintrag in der NAT-Tabelle:

WinRoute überprüft den gesamten ein- und ausgehenden Datenverkehr des LAN. Unabhängig davon, ob WinRoute NAT an einem bestimmten Paket ausführen soll oder nicht, wird das Paket zunächst untersucht und bestimmte Daten wie die Anschlussnummer und die IP-Adresse in die NAT-Tabelle eingetragen. Wenn die Pakete zurückkommen, kann WinRoute diese so mit der NAT-Tabelle vergleichen, um zu bestimmen, an wen das Paket zurückgeleitet werden muss. Wenn das Paket nicht initiiert ist, das heißt kein zurückkommendes Paket ist, vergleicht WinRoute es mit der NAT-Tabelle und stellt fest, dass es nicht initiiert ist. Wenn keine Anschlusszuordnungen erstellt sind, kann WinRoute das Paket nicht an einen Teilnehmer im lokalen Netzwerk senden.

- Mit der Option "abgelehntes Paket senden" wird das Paket mit der Nachricht an den Absender zurückgesandt, dass keine Verbindung erstellt werden konnte.

- Mit der Option "Paket abwerfen (automatische Installation)" wird das Paket vernichtet und kein Paket zurückgesandt. Auf diese Art und Weise werden keine Hinweise auf die Existenz des WinRoute-Host sowie des entsprechenden LANs nach außen gegeben.

Eingehende UDP-Pakete:

Bei einigen Anwendungen, die das **User Datagram Protocol** (UDP) verwenden ist es erforderlich, UDP-Pakete an einen zentralen Server zu senden. WinRoute zeichnet die Quelle und den Bestimmungsort aller UDP-Pakete auf, die an den Server geleitet werden, der von der das Paket sendenden Anwendung zugewiesen wurde. In einigen Fällen leitet der Server Ihre IP und den Anschluss an einen anderen Computer weiter, von dem Sie dann ein UDP-Paket mit den angeforderten Informationen erhalten. Auch wenn dieser willkürlich gewählte Computer eine andere IP-Adresse als der Server besitzt, kann er dennoch UDP-Pakete in Ihr lokales Netzwerk senden, da er die entsprechende IP und den Anschluss kennt.

- Bleiben wir bei diesem Beispiel. Wenn Sie *“kann NAT mit einer beliebigen IP-Quelladresse passieren"* wählen, werden UDP-Pakete durch WinRoute transportiert.
- Um die Sicherheit zu verbessern, wählen Sie die Option “*kann NAT nur passieren, wenn es von der IP-Quelladresse stammt, die beim Versenden des ersten ausgehenden Pakets registriert wurde*” wählen. Mit dieser Einstellung können nur UDP-Pakete vom zentralen Server WinRoute passieren.

NAT-Protokolloptionen:

Zu den erweiterten Sicherheitsoptionen gehört die Fähigkeit, Daten von Paketen, die in das LAN gelangen ohne von diesem angefordert worden zu sein, zu erfassen. Dies betrifft in der Regel Netzwerke, die Web, FTP, DNS oder eine andere Art von Server hinter WinRoute ausführen. Diese Funktion ist hilfreich, um die Ursache des Problems zu bestimmen.

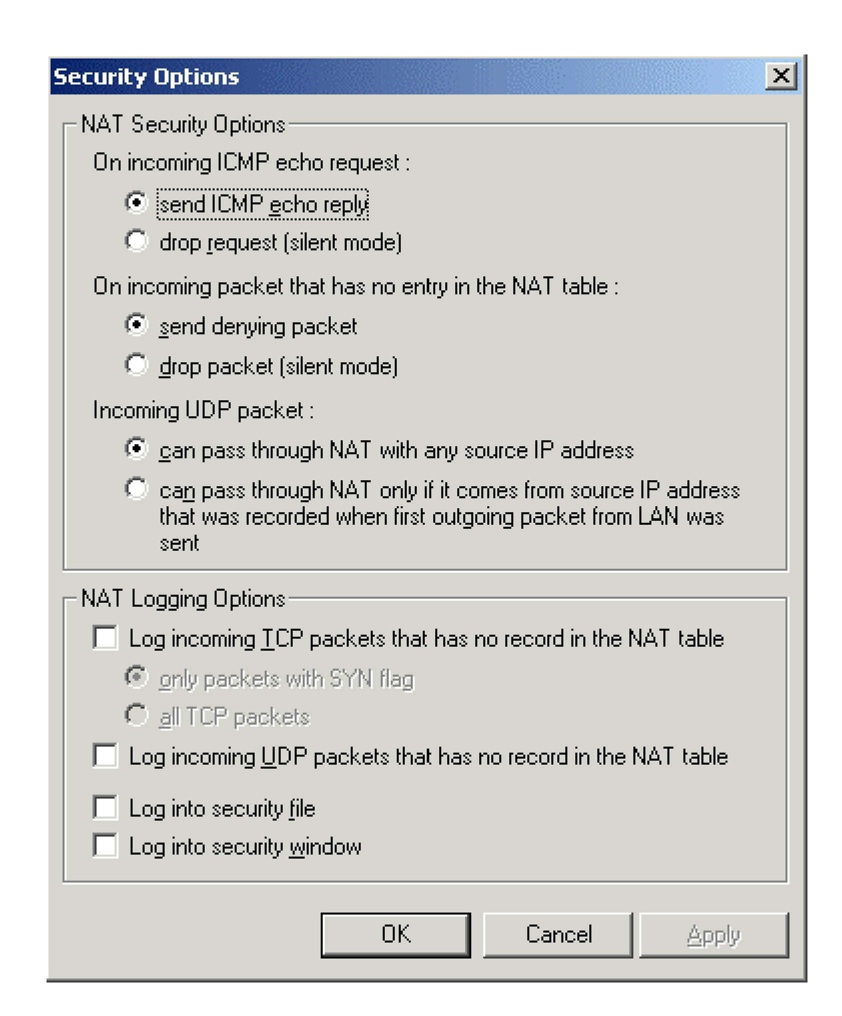
Protokollierung eingehender Pakete ohne Eintrag in die NAT-Tabelle:

WinRoute bietet zwei Möglichkeiten, TCP-Pakete zu protokollieren, die nicht in der NAT-Tabelle enthalten sind.

- Wenn Sie "*nur Pakete mit SYN-Flag*" (synchronisieren) protokollieren möchten, wird das TCP-Paket nur protokolliert, wenn eine Verbindung zwischen dem Absender und dem Empfänger hergestellt wurde.
- Mit der Option "*alle TCP-Pakete*" werden alle eingehenden TCP-Pakete protokolliert, und zwar unabhängig davon, ob eine Verbindung erstellt wurde. Da die UDP-Pakete keine Flags (Merker) verwenden, werden alle nicht initiierten UDP-Pakete protokolliert, sofern Sie UDP-Pakete protokollieren möchten.

Protokollieren in eine Datei oder ein Fenster:

- Wenn Sie "*In Sicherheitsfenster protokollieren*" auswählen, können Protokollinformationen in der WinRoute-Anwendung Administration anzeigen, indem Sie "Protokolle anzeigen" und "Sicherheitsprotokoll" wählen.
- Wenn Sie "*Protokollieren in eine Datei*" auswählen, speichert WinRoute die Protokollinformationen in das Sicherheitsprotokoll im Protokollordner von WinRoute Pro (in der Regel c:/Program Files/WinRoute Pro/Logs)


Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

Paketfilter-Einstellungen

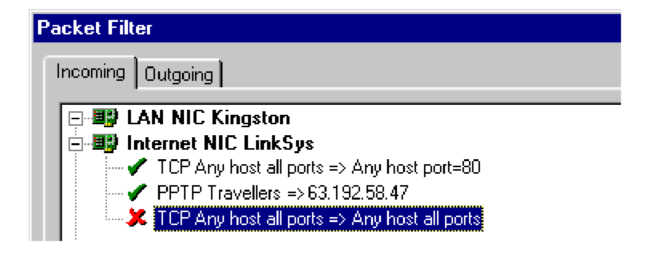
Die Konfiguration des Paketfilters der Firewall von WinRoute Pro ist sehr einfach. Dennoch ist ein gutes Verständnis der hinter der Paketfilter-Funktion stehenden Logik, wie diese in WinRoute angewandt wird, erforderlich.

Für die einzelnen Schnittstellen festgelegte Regeln

Benutzer können separate Sicherheitsregeln für individuelle Computerschnittstellen festlegen. Dies ist eine wichtige Funktion bei der Verwaltung von Netzwerken mit mehreren Segmenten.

Im folgenden Beispiel ist ein Netzwerk dargestellt, das:

- *jeder Person im Internet erlaubt, auf den Webserver innerhalb des Netzwerks zuzugreifen.*
- es *nur bestimmten Personen innerhalb der vordefinierten Adressengruppe mit der Bezeichnung "Travellers" erlaubt, auf den PPTP-Server innerhalb des Netzwerks zuzugreifen, um in das Netzwerk zu gelangen.*

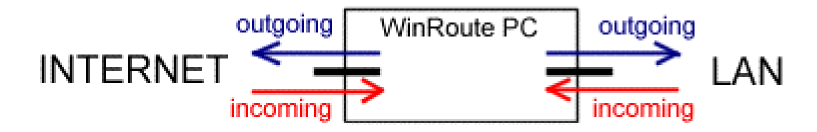


Unterschiedliche Regeln für ausgehende und eingehende Pakete

WinRoute wendet spezielle Regeln für ausgehende und eingehende Paket an. Innerhalb von WinRoute wird eine Tabelle für jede Schnittstelle erstellt. In dieser Tabelle werden sowohl die eingehenden als auch die ausgehenden Pakete erfasst. Mit anderen Worten, jedes Paket erhält zwei Einträge - einen für "ausgehend" und einen für "eingehend".

Was bedeutet AUSGEHENDES/EINGEHENDES Paket?

In WinRoute wird die Engine als Zentrum des gesamten Systems betrachtet. Dies bedeutet, dass alle Pakete, die WinRoute verlassen, AUSGEHENDE Pakete sind, und zwar unabhängig davon, ob sie in das Internet oder in das LAN gesendet werden. Ebenso werden alle Pakete, die ZUM WinRoute-Computer geleitet werden, als EINGEHEND angesehen, unabhängig davon, woher sie kommen. Dies muss beim Festlegen der Sicherheitsregeln beachtet werden.



Anwendung der Regeln

Von OBEN nach UNTEN

Die Regeln werden in einer Liste festgelegt und von oben nach unten angewandt. Wenn ein Paket an der Schnittstelle ankommt, wird es auf die in der Liste vorhandenen Regeln hin überprüft. Die Prüfung beginnt mit der ganz oben stehenden Regel und endet mit der Regel ganz unten. Treffen die Regeln auf das Paket zu, wird die Regel angewandt und die nachfolgenden werden ignoriert.

Regeln können auf Folgendes angewandt werden:

- einzelne Benutzer
- einen IP-Adressenbereich

- eine benutzerdefinierte Gruppe von IP-Adressen (um eine Gruppe von Benutzern festzulegen, sehen Sie im Referenzteil dieses Handbuches nach)
- das gesamte Teilnetz oder Netzwerk



Regeln können in einer vordefinierten Zeitzone angewandt werden

In einigen Fällen kann es nützlich sein, spezielle Regeln während der Bürozeiten und andere Kriterien für den Zugriff in der Zeit nach Büroschluss anzuwenden. Sie können auch bestimmten Benutzern den Zugang während der Mittagspause gestatten und ihn während der Arbeitszeit auf bestimmte Internetressourcen beschränken.

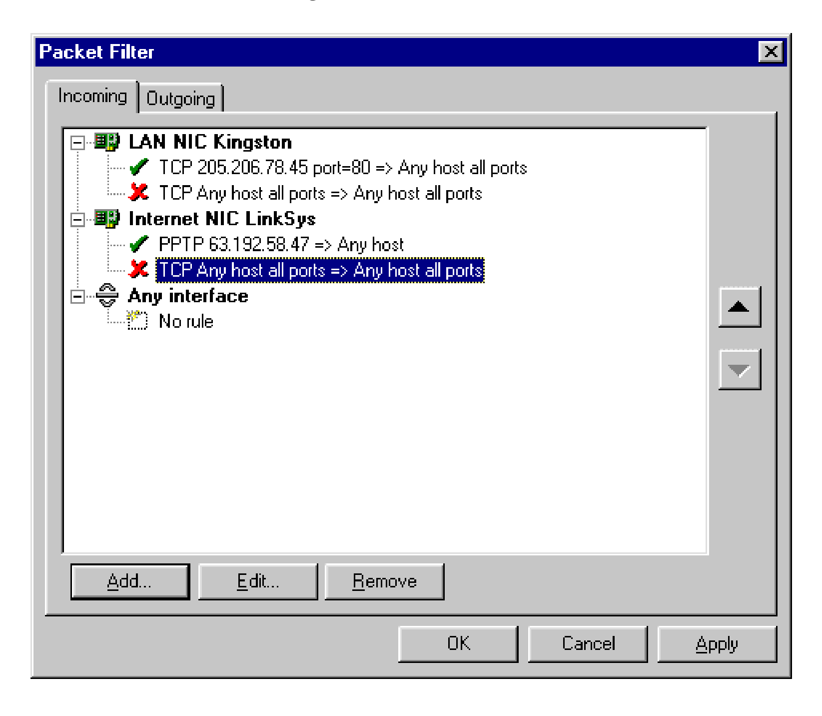
Beispiel

Vollständige Kontrolle des Benutzerzugangs: Der Netzwerkadministrator möchte, dass Benutzer Zugriff auf Ihr Netzwerk erhalten. Bei vielen Netzwerkinstallationen werden Web- oder FTP-Server hinter dem WinRoute-System ausgeführt, die öffentlichen Zugriff erfordern.

Im oben genannten Fall würde man die Regeln für eingehende Pakete in der folgenden Reihenfolge einstellen.

1. Pakete, die an Anschluss 80 gehen, von jedem Host zulassen.
2. Pakete, die an Anschluss 21 gehen, von jedem Host zulassen.
3. Alle Pakete ablehnen.

Wenn das ankommende Paket der Regel 1 oder 2 entspricht, wird das Paket durchgelassen und Regel 3 wird nicht angewandt. Entspricht das Paket Regel 1 oder 2 nicht, wird es abgelehnt.



Beispiel für ein Satz von Paketfilterkriterien

Regeln für eingehende Pakete (vergewissern Sie sich, dass sie dieser Reihenfolge entsprechen)

Protokoll	Quelle	Ziel	ICMP-Typen	Aktion	Protokollieren	
UDP	Jede beliebige Adresse, Anschluss = 53	Jede beliebige Adresse, Anschluss > 1023		Zulassen		
TCP	Jede beliebige Adresse, jeder beliebige Anschluss	Jede beliebige Adresse, Anschluss > 1023		Eingerichtetes TCP erlauben		
ICMP	Jede beliebige Adresse	Jede beliebige Adresse	Echo-Antwort	Zugriff erlauben		
IP	Jede beliebige Adresse	Jede beliebige Adresse		Verwerfen	in Fenster	

Hinweis: Diese letzte "Cleanup-Regel" greift in jedes Tool zur Paketüberwachung des Netzwerks ein, das auf diesem Host verwendet wird.

Musterbeispiel für einen Kriteriumssatz für Paketfilter bei eingehenden HTTP und FTP

Protokoll	Quelle	Ziel	ICMP-Typen	Aktion	Protokollieren	Be
TCP	Jede beliebige Adresse, jeder beliebige Anschluss	[dieser Host], Anschluss = 80		Zugang erlauben	(optional)	Err HT auf
TCP	Jede beliebige Adresse, jeder beliebige Anschluss	[dieser Host], Anschluss = 21		Zugang erlauben	(optional)	Err Ko die
TCP	Jede beliebige Adresse, jeder beliebige Anschluss	[dieser Host], Anschluss = 20		Zugang erlauben	(optional)	Err FT die pas Öf 10

Gewährung der Kommunikation an bestimmten Anschlüssen

Sie möchten folgende Regeln anwenden:

- maximale Sicherheit
- Zugriff auf Ihren Web-Server erlauben
- Kommunikation mit Ihrem SMTP-Server erlauben
- Abholung von E-Mail aus dem Internet über Ihren Mail-Server erlauben
- Zugriff auf Ihren FTP-Server erlauben

Maximale Sicherheit

Eingehend (Registerkarte)

Protokoll: TCP, alle eingehenden Pakete ablehnen

Quell-IP - Beliebig	Ziel-IP - Beliebig
Quellanschluss - Beliebig	Zielanschluss - Beliebig

Diese Regel ist unter den an der Schnittstelle verfügbaren Regeln immer die niedrigste.

Zugriff auf Ihren Web-Server erlauben

Eingehend (Registerkarte)

Protokoll: TCP

Quell-IP - Beliebig	Ziel-IP - IP-Adresse des Webservers
Quellanschluss - Beliebig	Zielanschluss - 80

Zugriff auf Ihren FTP-Server von bestimmten Adressen aus dem Internet erlauben.

Eingangs-Tab

Protokoll: TCP

Quell-IP -Beliebig	Ziel-IP - IP-Adresse des FTP-Servers
Quellanschluss - Beliebig	Zielanschluss - 21

Quell-IP - Beliebig	Ziel-IP - IP-Adresse des FTP-Servers
Quellanschluss - Beliebig	Zielanschluss - 20

Ihrem SMTP-Server nur die Kommunikation mittels Ihres Relay-SMTP-Servers erlauben (beim ISP)

Eingehend (Registerkarte)

Protokoll: TCP

Quell-IP - Relay-SMTP-Server des ISP	Ziel-IP - IP-Adresse des SMTP- Servers in Ihrem LAN
Quellanschluss - Beliebig	Zielanschluss - 25

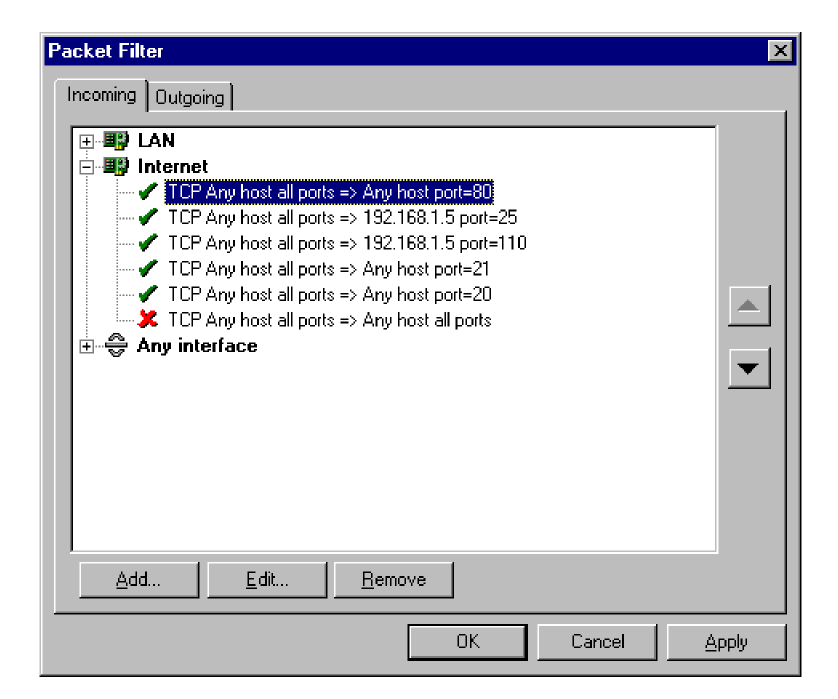
Ausgehend (Registerkarte)

Quell-IP - Ihr SMTP-Server	Ziel-IP - IP-Adresse des SMTP Servers beim ISP
Quellanschluss - Beliebig	Zielanschluss - 25

Ermöglicht es Ihnen, E-Mails aus dem Internet bei Ihrem Mail-Server abzuholen.

Eingehend (Registerkarte)

Quell-IP - Ihr SMTP-Server	Ziel-IP - IP-Adresse des SMTP-Servers Ihres LAN
Quellanschluss - Beliebig	Zielanschluss - 110


Packet Filter
Incoming
Outgoing
LAN
Internet
TCP Any host all ports => Any host port=80
TCP Any host all ports => 192.168.1.5 port=25
TCP Any host all ports => 192.168.1.5 port=110
TCP Any host all ports => Any host port=21
TCP Any host all ports => Any host port=20
TCP Any host all ports => Any host all ports
Any interface
Add...
Edit...
Remove
OK
Cancel
Apply

So veranlassen Sie die Benutzer dazu, den Proxy-Server zu verwenden

Unter Umständen empfiehlt es sich, den **integrierten PROXY-Server** von WinRoute zu verwenden. Dies ist hilfreich, wenn Sie die Aktivitäten der Benutzer beim Zugriff auf Webseiten **überwachen** möchten, für den Client-Zugriff auf bestimmte Websites **Einschränkungen anwenden** möchten oder wenn Sie möchten, dass diese den **Cache-Speicher** verwenden.

➢ ***Hinweis! Sie können*** *Paketfilter* ***verwenden, um den Datenverkehr im Netz zu überwachen; einfacher ist es jedoch, den*** *eingebauten Proxy-URL-Filter* ***einzusetzen, da dieser die Domänennamen auflöst. So müssen Sie nur den URL statt die zugeordnete IP-Adresse eingeben.***

Einstellungen

Erstellen Sie zwei Sicherheitsregeln für **ausgehende** Pakete:

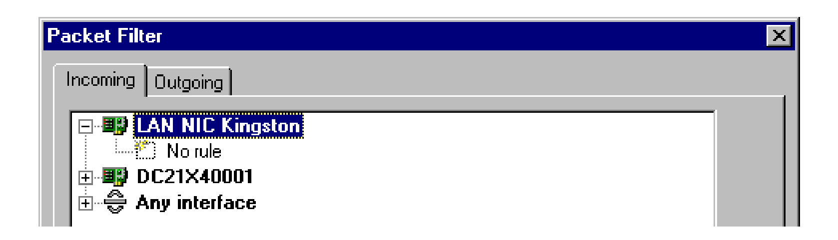
1. Ausgehende Pakete mit Zielanschluss 80 und der Quell-IP des WinRoute-Host **zulassen.**
2. Alle ausgehenden Pakete mit Zielanschluss 80 **ablehnen.**

Die Regeln müssen exakt in der oben erläuterten Reihenfolge angewandt werden. WinRoute wendet sie **von oben nach unten** an. Die Regeln auf der Basis "wer zuerst kommt malt zuerst" angewandt, d. h., eingehende Pakete werden von oben nach unten mit den Regeln verglichen, wobei die erste Regel oben und letzte Regel unten steht. Die erste Regel, die der Paketbeschreibung entspricht, wird angewandt, während die anderen Regeln ignoriert werden.

So konfigurieren Sie die Regeln:

1. Rufen Sie in WinRoute Administrator das Menü *Einstllungen=>Erweitert=>Paketfilter* auf. Klicken Sie auf die Registerkarte "Ausgehend".

2. Doppelklicken Sie auf Ihre externe (Internet-)Schnittstelle. Die Liste der Regeln oder "Keine Regel" wird angezeigt.



3. Klicken Sie auf die Schaltfläche *Hinzufügen,* um ein neue Regel hinzuzufügen, die den WinRoute-Host befähigen, Verbindungen mit Webservern an Anschluss 80 herzustellen.

Ausgewähltes Protokoll: TCP

Quell-Typ: Host

IP-Adresse: externe Adresse Ihrer WinRoute-Firewall (z. B. 204.23.43.26)

Zielanschluss: Gleich (=) 80, wählen Sie unter "Aktion" "zulassen".

4. Klicken Sie erneut auf die Schaltfläche *Hinzufügen*, um eine weitere Regel hinzuzufügen, mit der alle anderen TCP-Verbindungen mit Anschluss 80 abgelehnt werden.

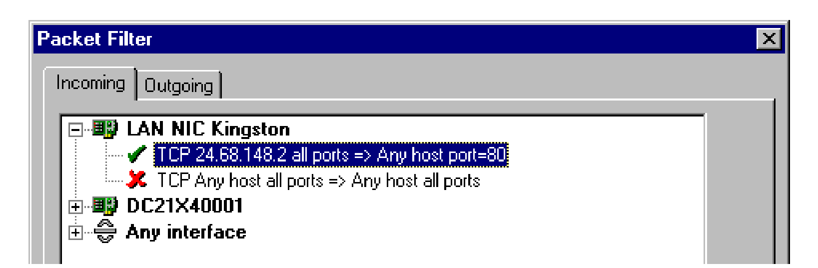
Ausgewähltes Protokoll: TCP

Quell-Typ: Beliebig

Zielanschluss: Gleich (=) 80

Aktion: Ablehnen.

Wenn Sie Versuche protokollieren möchten, aktivieren Sie das Kontrollkästchen "In Datei protokollieren".



- ***Hinweis: Wenn Sie zusätzliche Regeln konfigurieren, denken Sie daran, diese von OBEN nach UNTEN zu erstellen.***

Einrichten des MAIL-Servers

In diesem Abschnitt

Mail-Benutzer

Es bestehen einige Regelungen bezüglich der Benutzer, der E-Mail-Adressen und der Mailboxen in WinRoute.

Ein Benutzer = Eine Mailbox ...

Jeder Benutzer kann eine **Mailbox** erstellen. Die Mailbox enthält den Namen des Benutzers. Für den Fall, dass Sie in WinRoute eine Internetdomäne registriert und eingetragen haben, ist die E-Mail-Adresse automatisch Benutzer@Domäne.com.

Ein Benutzer = Mehrere Adressen

Sie können Aliasnamen festlegen, um verschiedene E-Mail-Adressen zu verwenden und allgemeine Postfächer wie Verkauf@...., Support@...., Info@.... einzurichten. Es gibt praktisch unendlich viele Kombinationsmöglichkeiten.

So fügen Sie einen Benutzer hinzu:

1 Öffnen Sie das Menü **Einstellungen=>Konten**

2 Fügen Sie **Benutzer** hinzu.

3 Fassen Sie gegebenenfalls die Benutzer in **Gruppen** zusammen.

Beispiel:

Das Unternehmen hat die Domäne brutus.com. Der Benutzer Thomas hat die E-Mail-Adresse Thomas@brutus.com. Weitere Informationen zu anderen Adressoptionen finden Sie unter Aliasnamen.

- ***Hinweis: Die Mailboxen werden in einem separaten Verzeichnis abgelegt, und zwar in der Regel in c:/Programmordner/WinRoute/Mail. Sie werden physisch erstellt, NACHDEM die erste E-Mail eingegangen ist.***

E-Mail-Versand an andere Benutzer von WinRoute innerhalb Ihres Netzwerks

Um E-Mails an andere Benutzer **innerhalb** Ihres LAN zu senden, verwenden Sie den **WinRoute-Benutzernamen** des Empfängers und nicht seine vollständige **Internet-E-Mail-**Adresse.

Beispiel: Der Name des Empfängers ist Thomas und seine vollständige E-Mail-Adresse lautet thomas@Unternehmen.com. Es reicht, wenn Sie nur *Thomas* in das Feld *An:* der E-Mail-Nachricht eingeben.

Thema Aliasnamen:

Wenn Sie die **vollständige E-Mail-Adresse** eines lokalen Benutzers eingeben, wird die Nachricht **durch** das Internet transportiert, d. h. zum Relay-SMTP-Server von WinRoute und dann zurück zu WinRoute. Um dies zu verhindern, müssen Sie Aliasnamen spezifizieren.

- ***Denken Sie daran! Sie müssen den WinRoute-PC als ausgehenden Mail-Server einrichten (STMP).***

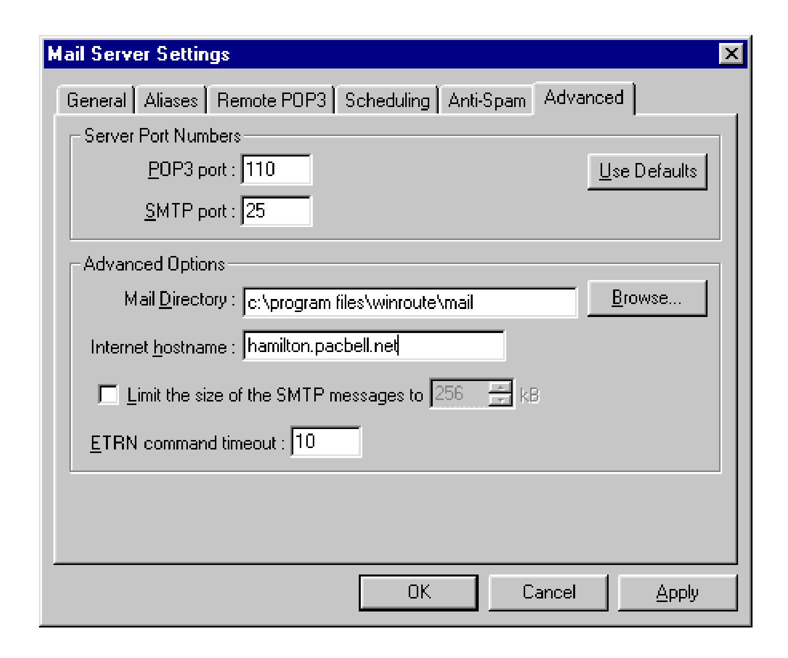
Authentifizierung

Authentifizierung

Einige Internetdiensteanbieter führen bei eingehenden E-Mails eine Authentifizierungsprüfung durch, um "Spamming" zu vermeiden. In diesem Fall müssen Sie Ihrem Diensteanbieter die entsprechenden Informationen zur Verfügung stellen.

1. Gehen Sie in das Fenster *Mail -Server->Register Erweitert.*

2. Geben Sie den gewünschten **Host-Namen** in das Feld für den Internet-Host-Namen ein. Üblicherweise ist dies der Name des Computers, der mit dem Internet verbunden ist (z. B. *host.isp.com)*.



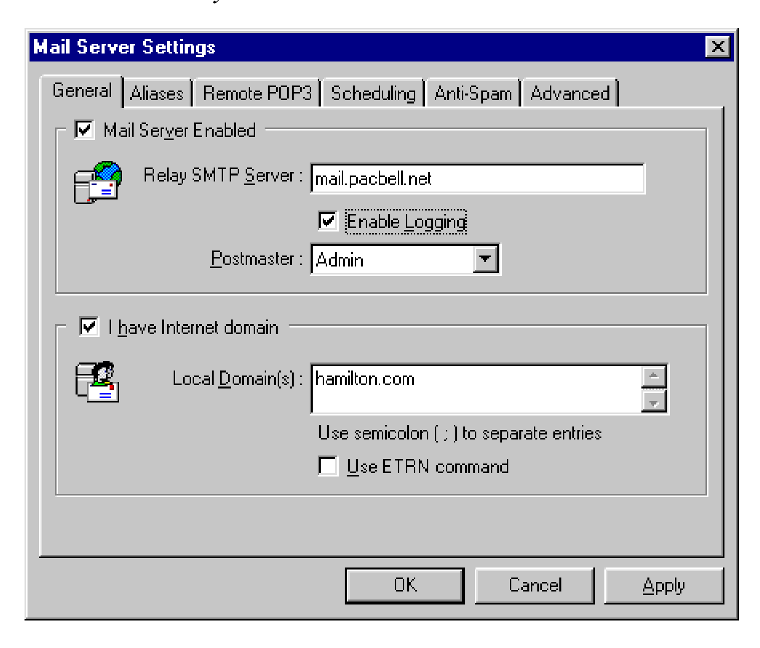
E-Mail-Versand in das Internet

Sie können WinRoute als Ihren **SMTP-Server** für ausgehende E-Mails verwenden. WinRoute sendet E-Mails über den **Relay- SMTP- Server** Ihres Diensteanbieters anwenden anstatt über MX-Record. Mit anderen Worten, alle ausgehenden E-Mails werden über den von Ihnen eingegebenen Mail-Server versandt (in der Regel ist dies der Mail-Server Ihres Internetdiensteanbieters). Dasselbe gilt für Ihre E-Mail-Clients, d. h. der WinRoute-Mail-Server kann als deren SMTP-Server fungieren.

So richten Sie den Relay-SMTP-Server für ausgehende E-Mails ein:

1 Öffnen Sie das Menü *Einstellungen=>Mail-Server*

2 Geben Sie den ausgehenden Mail-Server Ihres Diensteanbieters in das Feld für den *Relay-SMTP-Server* ein.

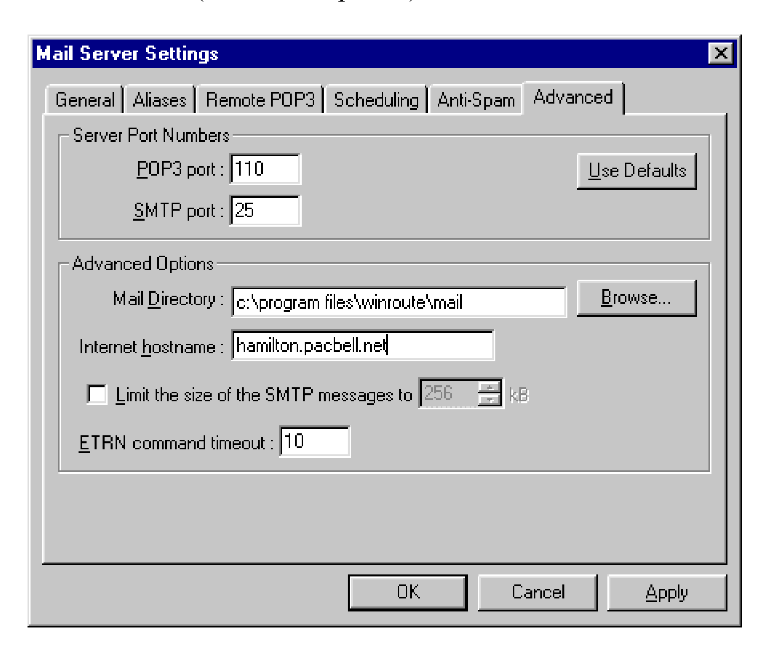


Authentifizierung

Einige Internetdiensteanbieter führen bei eingehenden E-Mails eine Authentifizierungsprüfung durch, um "Spamming" zu vermeiden. In diesem Fall müssen Sie Ihrem Diensteanbieter die entsprechenden Informationen zur Verfügung stellen.

1. Gehen Sie in das Fenster *Mail Server->Register Erweitert.*

2.Geben Sie den gewünschten **Host- Namen** in das Feld für den Internet-Host-Namen ein. In der Regel ist dies der Name des Computers, der mit dem Internet verbunden ist (z. B. *host.isp.com)*.



Aliasnamen

Aliasnamen werden in WinRoute verwendet, um Benutzern von WinRoute **zusätzliche** Adressen zuzuweisen sowie für die **Substitution** von E-Mail-Adressen.

Aliasnamen bieten folgende Möglichkeiten:

- mehrere Adressen für den gleichen Benutzer
- eine E-Mail-Adresse für mehrere Benutzer
- eine E-Mail-Adresse für eine Gruppe von Benutzern
- mehrere Adressen für eine Gruppe von Benutzern

Beispiel:

Das Beispiel zeigt, dass die Möglichkeiten unerschöpflich sind.

Das Unternehmen verfügt über 2 Domänen:

- Unternehmen.com
- Unternehmen2.com

Der Benutzer *Thomas* soll E-Mails empfangen für:

thomas_sprecher@unternehmen.com

thomas@unternehmen2.com

verkauf@unternehmen.com

support@unternehmen.com

Die E-Mail für *verkauf@unternehmen.co*m soll auch an die Gruppe *[Verkauf]* gesendet werden.

Lösung:

1. Öffnen Sie das Menü *Einstellungen=>Mail-Server=>Register Aliasname*n.

2. Fügen Sie folgende Aliasnamen hinzu:

*thomas** sendet an *Thoma*s -

Mit diesem Alias werden alle E-Mails aus dem Internet an Thomas als Empfänger gesandt. D.h., Mails an *thomas_Sprecher@unternehmen.co*m werden ebenso dem Benutzer *Thomas* zugestellt und Mails an *thomas@unternehmen2.co*m werden dem Benutzer zugestellt. Dies verhindert auch, dass E-Mails, die von lokalen Benutzern an den Empfänger *thomas@unternehmen.com* gesendet werden, durch das Internet transportiert werden. Sie werden direkt an das Postfach von *Thoma*s in WinRoute gesandt.

Verkauf sendet an *Thoma*s -

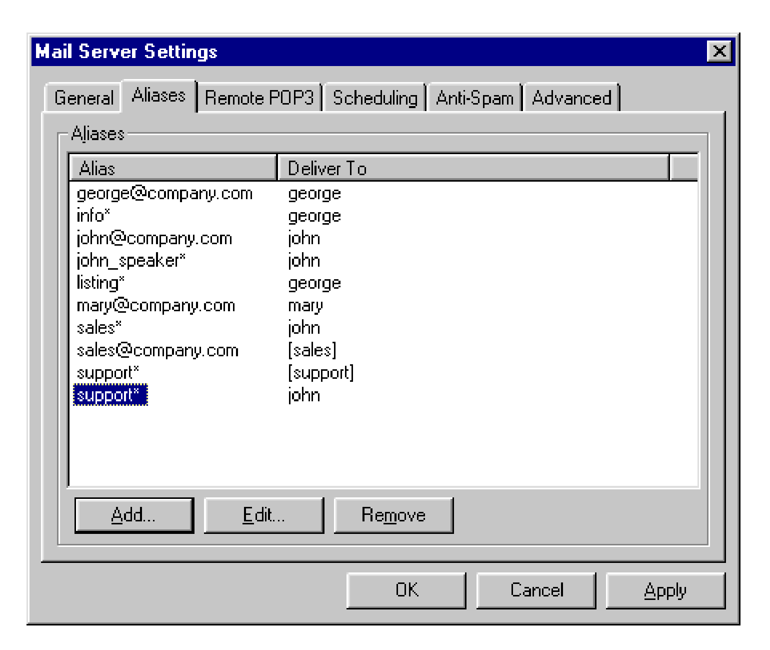
E-Mails an *Verkauf@……..* werden an den Benutzer *Thoma*s gesandt.

*Suppor*t sendet an *Thoma*s -

E-Mails an *Support@……* werden an *Thoma*s gesandt.

*Verkau*f sendet an *[Verkauf*] -

E-Mails an *Verkauf@….* werden an alle Mitglieder der Gruppe *[Verkauf]* gesandt.



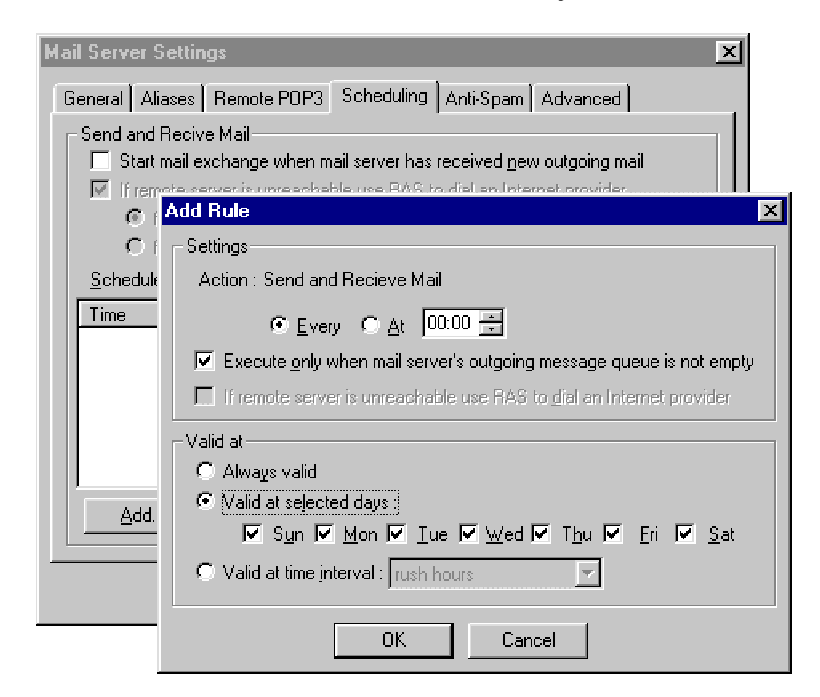
Zeitplan für den E-Mail-Austausch

Mit dem Zeitplan in den Einstellungen des Mail-Servers können Sie folgende Optionen festlegen:

- reguläre Zeitintervalle, in denen die E-Mails bei Ihrem Internetdiensteanbieters abgefragt werden (POP3 oder SMTP unter Verwendung von ETRN)
- Versandregeln für E-Mail
- Zeitintervalle, in denen die Regeln Gültigkeit haben. Sie können diese Intervalle im Menü *Einstellungen->erweitert->Zeitintervalle* vorab festlegen.

Sie können angeben, ob Sie ausgehende E-Mail sofort versenden möchten, nachdem diese auf dem Mail-Server angekommen sind, oder innerhalb eines bestimmten Zeitraums.

Sie können auch festlegen, ob der E-Mail-Server bei vorhandener neuen ausgehenden E-Mails hinauswählen soll oder nicht. Wenn Sie diese Option wählen, stellt der Mail-Server von WinRoute jedesmal, wenn einer der Benutzer eine neue E-Mail versendet, eine Verbindung her.



Für den Empfang von Nachrichten können Sie eine genaue Zeit angeben, wann Sie Ihre E-Mail abholen möchten. Durch die Kombination verschiedener Regeln lässt sich die Abholung Ihrer E-Mails so effizient wie möglich gestalten.

1 Öffnen Sie das Menü *Einstellungen->Mail-Server->Zeitplan*

2 Geben Sie die gewünschten Optionen an, und fügen Sie neue Regeln für E-Mails hinzu.

- ***Hinweis! Regeln für die "Zeitintervalle" müssen im Menü Einstellungen->Erweitert->Zeitintervalle festgelegt werden.***

Empfang von E-Mails

In diesem Abschnitt

Sie besitzen eine Domäne (SMTP)

Der Ma-Server von WinRoute ist vollständig mit ***SMTP***[1]/***POP3***[2] kompatibel. Sie können Ihre eigene registrierte **Internetdomäne** haben und E-Mail über SMTP empfangen und/oder WinRoute könnte E-Mail automatisch vom POP3-Konto Ihres Internetdiensteanbieters abholen.

---

[1] **SMTP** (Simple Mail Transfer Protocol) wird für die direkte Kommunikation zwischen den Mail-Servern (wie dem Mail-Server in WinRoute und den Mail-Server Ihres Diensteanbieters) verwendet sowie für den E-Mail-Versand über Ihre E-Mail-Client-Software. SMTP ist ein "Einweg"-Protokoll - d. h. der Mail-Server kann E-Mails versenden oder empfangen. Es ist jedoch nicht möglich, E-Mails bei einem anderen Mail-Server, der dieses Protokoll verwendet, abzuholen.

SMTP-Protokoll ist ein TCP-Protokoll, das an **Anschluss 25** ausgeführt wird. Wenn Sie auf dieses Protokoll mit dem Mail-Server, der hinter oder am WinRoute-Computer ausgeführt wird, zugreifen möchten (um anderen Mail-Servern das Recht einzuräumen, Ihnen E-Mails zu senden oder um diesen Mail-Server für den Versand Ihrer E-Mails einzusetzen, wenn Sie sich in Ihrem LAN befinden), müssen Sie die **Anschlusszuordnung** für das TCP-Protokoll durchführen. Anschluss 25 sendet die E-Mails an die **private** IP-Adresse des PCs, auf dem der Mail-Server ausgeführt wird.

[2] **POP3-**Protokoll wird meistens von E-Mail-Client-Software verwendet, um die E-Mail von den Postfächern der mit POP3 kompatiblen Mail-Servern abzuholen. Auch der Mail-Server von WinRoute verfügt über eine solche Funktion. Das bedeutet, er kann die E-Mail automatisch bei jedem mit POP3 kompatiblen Mail-Server abholen und diese weiter an die Postfächer lokaler Empfänger verteilen.

POP3-Protokoll ist ein **TCP-**Protokoll, das an **Anschluss 110** ausgeführt wird. Wenn Sie auf diesen Protokoll-Mail-Server zugreifen möchten, der hinter oder auf dem WinRoute-Computer ausgeführt wird, (um Ihre E-Mail AUS dem Internet abzuholen), müssen Sie die **Anschlusszuordnung** für das TCP- Protokoll durchführen. Anschluss 110 sendet die E-Mails an die **private** IP-Adresse des PCs, der den Mail-Server ausführt.

Wenn Sie eine Internetdomäne für Ihre externe (öffentliche) IP-Adresse registriert haben, kann WinRoute E-Mail mit dem SMTP-Protokoll empfangen.

➢ ***Vergessen Sie nicht den Anschluss 25 des TCP-Protokolls der privaten IP-Adresse Ihrer WinRoute-Mailbox zuzuordnen! Andernfalls wird es dem SMTP-Protokoll nicht ermöglicht, durch die NAT von WinRoute zu laufen!***

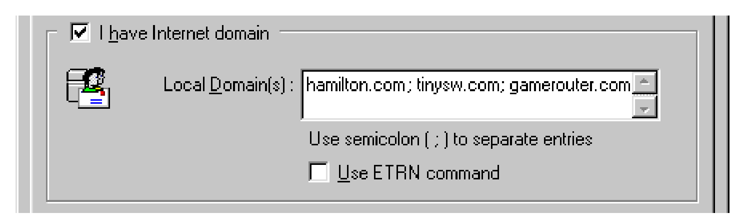
Je nachdem, welche Internetverbindung Sie besitzen ist Folgendes in Betracht zu ziehen:

1 Sie haben eine Standleitung

Hier sind keine speziellen Einstellungen erforderlich. Es werden lediglich die Domänen eingetragen.

2 Sie haben eine DFÜ- oder ISDN-Leitung (ETRN-Befehl)

Falls Sie keine Standleitung besitzen, wird Ihre E-Mail temporär bei Ihrem Internetdiensteanbieter gespeichert. Die E-Mail wird übertragen, wenn eine Verbindung hergestellt wird. Einige Anbieter verlangen, dass ein ***ETRN***[3]-Befehl verwendet wird, um E-Mails abzufragen. Der Mail-Server von WinRoute unterstützt den ETRN-Befehl. Sie können die Option in der Registerkarte *Allgemein* des Dialogfeldes des **Mail-Servers** aktivieren.



[3] ETRN ist ein vom SMTP-Server verwendeter Befehl, um eine Zeitverlängerung herzustellen/zu vereinbaren. Nachdem der SMTP-Server eine Verbindung hergestellt hat, sollte dieser eine Anfrage für SMTP-Mail ausführen.

Der ETRN-Befehl wird überall dort verwendet, wo ein SMTP-Server nicht 24 Stunden "online" ist und die E-Mails für solche Server in einem Zwischenspeicher eines anderen SMTP-Servers gespeichert werden müssen.

Falls erforderlich, können Sie einen ETRN-Zeitüberschreitungsintervall festlegen (rufen Sie die Registerkarte *Erweitert*).

Mail Server Settings

General | Aliases | Remote POP3 | Scheduling | Anti-Spam | Advanced

Server Port Numbers

POP3 port : 110 — Use Defaults

SMTP port : 25

Advanced Options

Mail Directory : c:\program files\winroute\mail — Browse...

Internet hostname : hamilton.pacbell.net

Limit the size of the SMTP messages to 256 kB

ETRN command timeout : 10

OK | Cancel | Apply

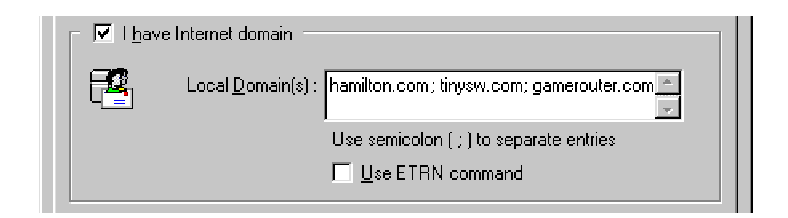
Zeitüberschreitung des ETRN-Befehls

Dieser Eintrag gibt an, wie viele Male der SMTP-Server von WinRoute eine Anfrage an SMTP-Mail richten soll, nachdem eine Verbindung erstellt wurde.

Mehrere Domänen

Mehrere Domänen

Ihrer Internetverbindung können mehrere Domänen zugewiesen sein. Falls Sie mehrere Domänen besitzen, geben Sie alle im Menü *Einstellungen=>Mail-Server=>Registerkarte Allgemein* ein, und trennen Sie diese durch einen Semikolon.



Relevante Themen im Zusammenhang mit mehreren Domänen:

Sie können Ihrem Netzwerk mehrere Domänen auf zwei Arten zuweisen:

1 Jede Domäne wird mit der eigenen IP-Adresse assoziiert.

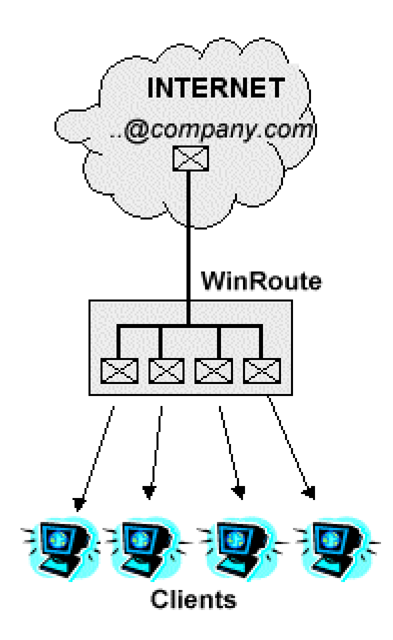
In diesem Fall müssen Sie mehrere öffentliche IP-Adressen der Schnittstelle zuordnen, die von WinRoute für die Internetverbindung verwendet wird. Vergeben Sie anschließend mehrere Einstellungen für die Anschlusszuordnung - eine für jede IP-Adresse - mit derselben IP-Zieladresse des WR-Computers.

2 Alle Domänen sind mit einer IP-Adresse assoziiert.

Hier ist lediglich eine Einstellung erforderlich, und zwar die Einrichtung einer Anschlusszuordnung für das TCP-Protokoll an Anschluss 25 zur IP-Adresse Ihres WinRoute-Computers.

Sie besitzen eine dem POP3-Konto zugewiesene Domäne

Sie können mit Ihrem Diensteanbieter vereinbaren, dass die gesamte E-Mail für Ihre Domäne in einem einzigen Konto eingeht. WinRoute kann ein solches Konto überprüfen, die Nachrichten abholen und diese automatisch an die E-Mail-Eingänge Ihrer lokalen Benutzer verteilen.



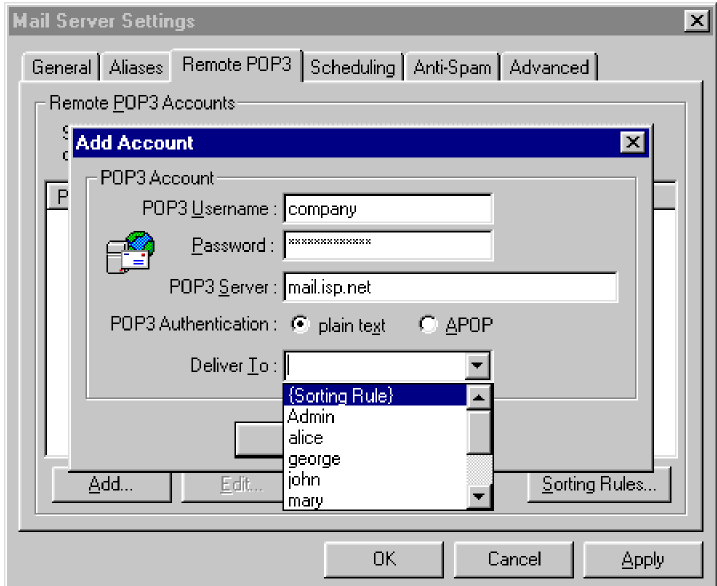
Beispiel

Ihr Diensteanbieter hat eine E-Mail-Konto Unternehmen@mail.isp.net eingerichtet. Auch wenn Sie möglicherweise die Domäne Unternehmen.com besitzen, gehen alle E-Mails für Ihre Domäne (Sales@Domain.com, john@Domäne.com) an Ihr Konto Unternehmen@mail.isp.net bei Ihrem Diensteanbieters.

1 Öffnen Sie das Menü *Einstellungen=>Mail-Server=>Fern-POP3*, fügen Sie ein neues Konto hinzu, und geben Sie die Informationen ein.

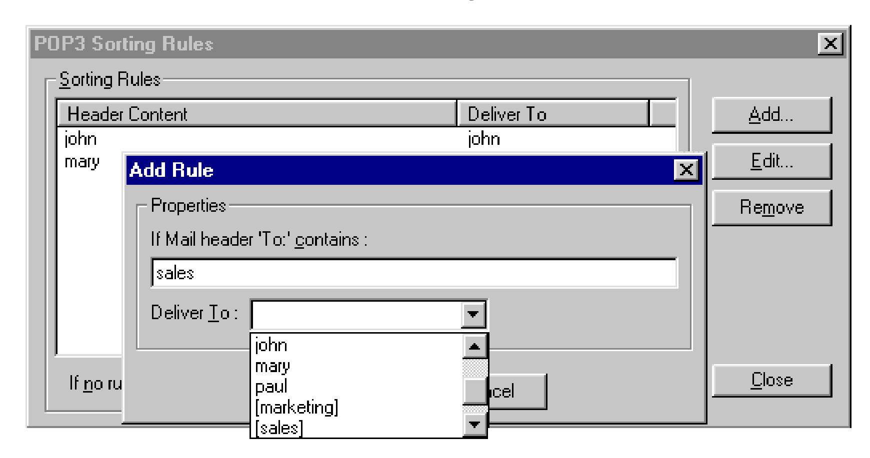


2 Im Feld "Senden an:" wählen Sie "Kriterien auswählen"



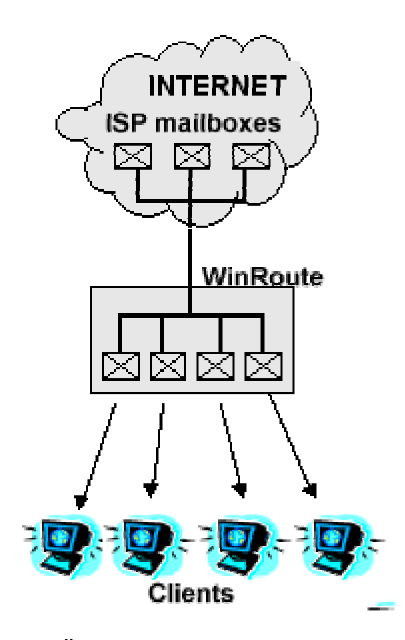
3 Aktivieren Sie die Schaltfläche "Kriterien auswählen", und fügen Sie ein neues Kriterium hinzu. WinRoute wird die E-Mail anhand der E-Mail-Adresse des Empfängers, Senders oder des Betreffs zustellen.

4 Wählen Sie im selben Dialogfeld einen Benutzer oder eine Gruppe von Benutzern aus, an die die E-Mail gesendet werden soll.



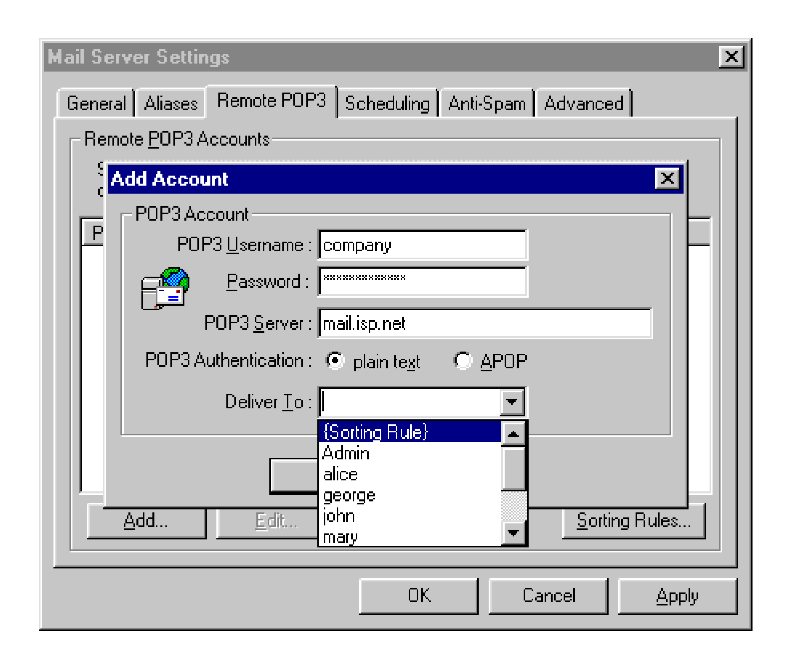
E-Mail empfangen - Sie haben mehrere Mailboxes bei Ihrem ISP

WinRoute ist in der Lage verschiedene Konten bei den verschiedenen Diensteanbietern zu überprüfen und automatisch die erhaltene E-Mail an die lokalen Empfänger senden.



1 Öffnen Sie das Menü *Einstellungen=>Mail-Server=>Fern-POP3*, fügen Sie ein neues Konto hinzu, und geben Sie die entsprechenden Informationen ein.

2 Im Feld für "Senden an:" wählen Sie den Empfänger oder die Gruppe von Empfängern aus.



Softwareeinstellungen für den E-Mail-Client

In diesem Abschnitt

WinRoute Mail-Server

E-Mail über den Mail-Server von WinRoute

Um den Mail-Server von WinRoute zu verwenden, müssen Sie Ihre **E-Mail-Client-Software** konfigurieren. Der WinRoute-Computer wird als Mail-Server für **eingehende** und **ausgehende Mails** fungieren. Daher ist es erforderlich, dass Sie den Namen des WinRoute-Computer in das richtige Feld Ihrer E-Mail-Software eingeben. Wenn Sie Schwierigkeiten haben, E-Mails zu senden oder zu empfangen, empfehlen wir Ihnen vorerst, die IP-Adresse anstelle des Computernamens einzugeben. Manchmal liegt das Problem in der DNS-Auflösung Ihres lokalen Netzwerks. Es kann der Anschein erweckt werden, als würden Sie den WinRoute DNS-Server nicht verwenden.

Beispiel:

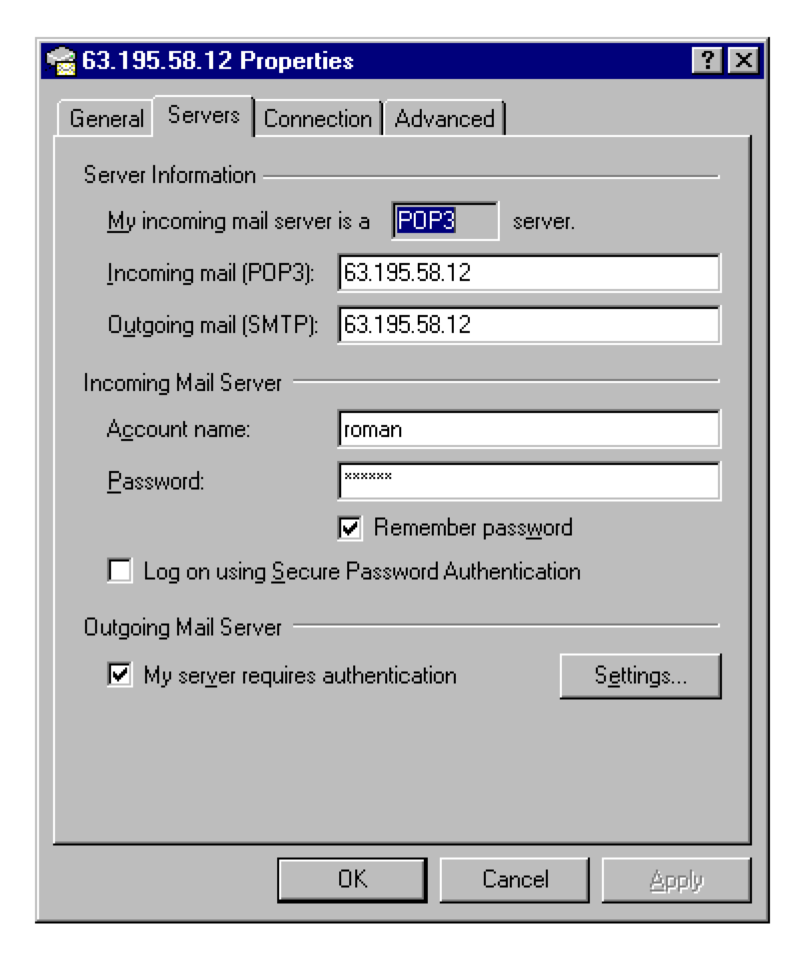
Der WinRoute Mail-Server wird auf einem Computer ausgeführt, der über eine automatisch zugewiesene öffentliche IP-Adresse verfügt oder über eine private IP-Adresse mit 192.168.1.1. Der Name des Computers ist Hamilton (siehe Systemsteuerung zur Netzwerkkontrolle).

Sie können entweder HAMILTON oder 192.168.1.1 in die Felder des Mail-Servers für eingehende (POP3) oder ausgehende (SMTP)-Mails in Ihrer E-Mail-Software eingeben.

So umgehen Sie den Mail-Server von WinRoute

Es kann sein, dass Sie den Mail-Server von WinRoute umgehen möchten, und E-Mail direkt mit einen E-Mail-Client über den Mail-Server Ihres Diensteanbieters empfangen oder senden wollen.

In diesem Fall geben Sie bitte den richtigen Namen des Mail-Servers Ihres Diensteanbieters in den Einstellungen für ausgehende und eingehende E-Mails ein.



- ***Hinweis! Konfigurieren Sie Ihre E-Mail-Client-Software so, dass der Proxy NICHT verwendet wird! Sie müssen die NAT von WinRoute für den Internetzugang verwenden und Ihre Client-Software so einrichten, dass eine direkte Verbindung zum Internet besteht. Sollte es nicht möglich sein E-Mails zu versenden bzw. zu empfangen, ist möglicherweise NAT nicht richtig konfiguriert. Folgen Sie den Anweisungen in der*** Checkliste ***, um NAT richtig zu konfigurieren!***

KAPITEL 3

EINSATZBEISPIELE

In diesem Kapitel

IPSEC-, NOVELL- und PPTP VPN-Lösungen

In diesem Abschnitt

IPSEC VPN

WinRoute Pro 4.1 unterstützt IPSEC im so genannten "**Tunnel-Modus**". Der "**Tunnel-Modus**" sollte jeden IPSEC-Client unterstützen, mit dem die Transport-IP-Adresse verändert werden kann.

Hinweis: WinRoute unterstützt keine Checkpoint Secure Remote VPN-Client-Software.

WinRoute-Einstellungen:

Zugeordneten Anschluss für ESP erstellen:

Protokoll: ungleich 50

Überwachungs-IP: <nicht spezifiziert>

Ziel-IP: die private IP-Adresse des Client-PC

Wir empfehlen außerdem, einen zugeordneten Anschluss für IKE zu erstellen. Dies ist nicht notwendig, wenn die Kommunikation HINTER WinRoute aus zum Internet initiiert wird. Manche Implementierungen von ISPC können unter Umständen jedoch folgende Einstellung erfordern:

IKE-Anschlusszuordnung:

Protokoll: UDP

Überwachungs-IP: <nicht spezifiziert>

Überwachungsanschluss: 500

Ziel-IP: die private IP-Adresse des Client-Computers

Zielanschluss: 500

Simultane Ausführung mehrerer IPSEC-Sitzungen

Wenn mehrere IPSEC-Clients vorhanden sind, müssen Sie für jeden Client eine separate IP-Adresse verwenden. Hinweis: WinRoute NAT lässt so viele Clients passieren, wie Sie möchten, sofern die Verbindung VOM lokalen Netzwerk aus initiiert wird und jeder Client eine IP-Adresse verwendet, die der externen Schnittstelle von WinRoute zugewiesen ist.

Allgemeine Informationen zu IPSEC

IPSec ist ein Sicherheitsprotokoll zur Verschlüsselung, mit dem die Kommunikation zwischen zwei Computern sicher gestaltet wird.

IPSec verwendet entweder AH (Authentification Header) oder ESP (Encapsulating Security Payload). AH überprüft lediglich die Identität des Senders und den Inhalt des Pakets. Die Daten werden nicht verschlüsselt.

ESP verschlüsselt die Daten. Es ermöglicht die Verwendung des so genannten "Tunnel-Modus", der dem PPTP-Protokoll ähnelt. Das Paket beinhaltet dann den IP-Header (für den Transport erforderlich), der nicht verschlüsselt ist, und den Datenteil, der das gesamte, verschlüsselte Originalpaket enthält.

Das Protokoll-IKE (mitunter als ISAKMP bezeichnet) wird für die Echtheitsbestätigung verwendet (Austausch von Sicherheitsschlüsseln). IKE wird am UDP-Protokoll Anschluss 500 ausgeführt. Dieser Anschluss wird als Quell- und Zielanschluss verwendet.

AH verwendet Protokoll 51, ESP das Protokoll 50. IPSec kann weiterhin mit der gesamten Zertifizierungsstelle kommunizieren, wenn Protokolle verwendet werden, die nicht in NAT eingreifen.

Das Protokoll 50 wird automatisch in WinRoute integriert, so dass keine Anschlusszuordnung notwendig ist. Die einzige Voraussetzung, um eine Verbindung automatisch herzustellen, wäre dann die Initialisierung der Verbindung VOM lokalen Netzwerk aus.

Die meisten Anbieter von IPSec verwenden den Algorithmus MD5 und SHA1 für die Echtheitsbestätigung und DES, 3DES und Blowfish für die Verschlüsselung. IPSec ist nicht eng mit einem speziellen Algorithmus verbunden, so dass die Lösungen verschiedener Anbieter inkompatibel sein könnten.

Novell Border Manager VPN

Verwenden von WinRoute Pro in Verbindung mit Novell BorderManager VPN (IPSEC)

Dieses Dokument beschreibt die Einstellungen, mit denen ein lokales Netzwerk, das NAT anwendet, so verbunden werden kann, dass eine IP-Adresse, die vom ISP an ein entferntes Netzwerk geliefert wird, welches Novell BorderManager Enterprise Server für die VPN-Konnektivität verwendet, gemeinsam genutzt wird.

Gemäß der README.TXT-Datei, die auf der Installationsdiskette des Novell BorderManager VPN-Client mitgeliefert wird,

"Können Sie NAT auf dem Pfad zwischen einem VPN-Client und einem VPN-Server nicht anwenden. Dies ist der Fall, wenn die IP- und IPX-Pakete am VPN-Client gekapselt und verschlüsselt sind und daher die IP-Quelladresse, die für die Kapselung genutzt wird, die Adresse des VPN-Client ist. Die Kalkulation für den Autorisierungs-Header von IPSEC basiert auf dieser Adresse und der Adresse des Ziel-VPN-Servers. Daher schlägt die Kalkulation, wenn eine der Adressen (VPN-Client oder VPN-Server) durch NAT modifiziert wird, bei Ankunft am Ziel-VPN-Server fehl, und das Paket wird nicht berücksichtigt. Es ist jedoch sehr wahrscheinlich, dass NAT die IPSEC-Pakete verwirft, da NAT nur TCP-, UDP- und Internet Control Message Protocol (ICMP)-Pakete bearbeitet.

Wenn Sie über Workstations innerhalb eines Intranets verfügen, die auf sichere Weise geschützt durch einen VPN-Server mit anderen Netzwerken über das Internet kommunizieren müssen, schlagen wir Ihnen vor, die Site-to-Site VPN-Funktion der Novell Border Manager Enterprise-Edition zu verwenden (anstelle der Client-to-Site VPN)."

Der Novell Border Manager Enterprise-Server ist jedoch sehr teuer für Privatbenutzer. Hinzu kommt, dass ein die erweiterten Einstellungen der statischen Routen des entfernten Netzwerks, auf das zugegriffen wird, notwenig sind. Die oben genannte Lösung von Novell ist daher nicht geeignet, wenn man sein lokales Netzwerk, das NAT verwendet, mit dem Novell Border Manager VPN mit einem entfernten Netzwerk verbinden will.

Interessanterweise ist es möglich, das lokale Netzwerk, das NAT verwendet, mit einem entfernten Netzwerk, welches WinRoute Pro und den Novell Border Manager VPN-Client verwendet, zu verbinden. Diese Konfiguration erlaubt es jedem Computer auf dem lokalen Netzwerk, auf die Ressourcen des entfernten Netzwerks zuzugreifen, wenn der VPN-Tunnel auf dem Router-Computer eingerichtet wurde. Es ist keine Konfiguration des entfernten Netzwerks erforderlich.

Nachfolgend sind die für die Konfiguration des lokalen Netzwerks notwendigen Schritte aufgeführt.

Schritt 1: Installieren und konfigurieren Sie die Novell Border Manger Client-Sortware auf dem Computer, der als Router verwendet werden soll. Vergewissern Sie sich, dass die Verbindung zwischen dem entfernten Netzwerk ordnungsgemäß eingerichtet ist und auf die Ressourcen des entfernten Netzwerks zugegriffen werden kann.

Schritt 2: Installieren Sie WinRoute Pro auf dem Router-Computer. Gehen Sie entsprechend der im Handbuch für den Administrator enthaltenen Anweisungen bezüglich der Konfiguration von WinRoute Pro und den Computern des lokalen Netzwerks, die mit WinRoute Pro arbeiten sollen, vor. Verwenden Sie die für die gemeinsame Nutzung einer einzelnen IP-Adresse übliche Konfiguration. Vergewissern Sie sich, dass auf die Ressourcen des Internets von jedem Computer des lokalen Netzwerks aus zugegriffen werden kann.

Schritt 3: Wenn Sie auf die Ressourcen des entfernten Netzwerks zugreifen müssen, führen Sie den Novell Border Manager VPN-Client am Router-Computer aus, und melden Sie sich am entfernten Netzwerk an.

Dies wird durch die Architektur von WinRoute Pro möglich. Da es auf IPSEC-Niveau arbeitet, findet die Adress-Übersetzung statt, bevor die Pakete zum virtuellen Netzwerkadapter geleitet werden. Daher haben die an den VPN-Server gesendeten Pakete die tatsächliche IP-Quelladresse. Auf dem Rückweg durchlaufen die vom virtuellen Netzwerkadapter erhaltenen Pakete die Ebene der Adressübersetzung (NAT) und werden an den richtigen Computer des lokalen Netzwerks geleitet.

Die Einschränkungen dieser Einstellung liegen darin, dass die VPN-Anmeldung manuell am Router-Computer vorgenommen werden muss, und dass die VPN-Verbindung gemäß der Einstellung am VPN-Server beendet wird, wenn sie eine gewisse Zeit nicht aktiv war. Auch IPX-Pakete werden nicht weitergeleitet, selbst wenn am VPN-Computer ein IPX-Protokoll aktiviert ist. Daher wird ein IPX-Tunneling nur am Router-Computer möglich sein.

Insgesamt bietet diese Einstellung einen kosteneffizienten und geeigneten Weg, ein lokales Netzwerk, das NAT verwendet, mit einem entfernten Netzwerk zu verbinden, das Novell Border Manager VPN benutzt.

Ausführen eines PPTP-Servers hinter NAT

Um einen PPTP-Server auf dem Netzwerk hinter WinRoute auszuführen (einschließlich Computer, auf denen WinRoute ausgeführt wird), müssen Sie die Anschlusszuordnung einrichten.

Wichtig: Wenn sich der VPN-Server auf der WinRoute Host-Maschine befindet, müssen Sie die Ziel-IP der **öffentlichen Adresse** *zuordnen und nicht der privaten. Die Überwachungs-IP sollte nicht spezifiziert bleiben.*

Für die Kontroll-Verbindung:

- Protokoll: TCP
- Überwachungs-IP:

- Überwachungsanschluss: 1723
- Ziel-IP: IP-Adresse Ihres PPTP-Servers (z. B. 192.168.1.12)
- Zielanschluss: 1723

Für GRE (PPTP)-Pakete:

- Protokoll: PPTP
- Überwachungs-IP:
- Ziel-IP: IP-Adresse Ihres PPTP-Servers (z. B. 192.168.1.12)

Nach dem Einrichten der Anschlusszuordnung, wie oben beschrieben, können Sie Ihren PPTP-Server überall hinter WinRoute, EINSCHLIESSLICH des WinRoute ausführenden Computers, einrichten. Die Benutzer greifen auf Ihren PPTP-Server zu, indem Sie sich über die externe (öffentliche) IP-Adresse Ihres Netzwerks einwählen. Wenn die Pakete den WinRoute-Computer erreichen, werden diese automatisch an den richtigen Computer hinter der Firewall weitergeleitet.

Beispiele für PPTP-Lösungen

WinRoute ermöglicht einen sehr kostengünstigen Weg, ein eigenes WAN zwischen mit dem Internet verbundenen Niederlassungen einzurichten. Wir gehen davon aus, dass die Leser dieses Handbuchs über Grundkenntnisse im Bereich Netzwerk und WindowsNT verfügen.

Ein solches WAN lässt sich in einigen einfachen Schritten einrichten:

1. Überprüfen Sie die Umgebung:

   NT-Server an beiden Enden

   WinRoute Pro ist an beiden Enden installiert.

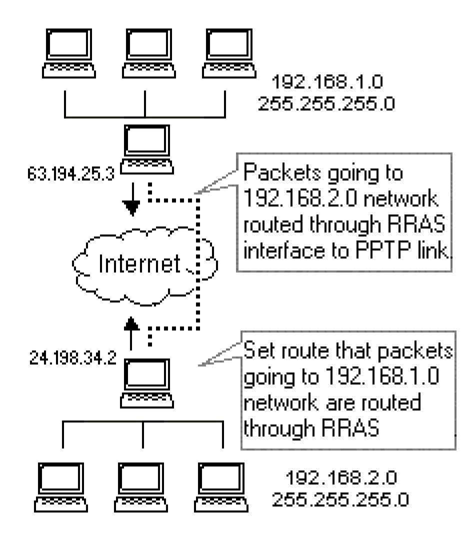
   RRAS (Stealhead) ist an beiden NAT-Servern installiert.

2. Erstellen Sie eine statische Route an beiden NT-Servern, die spezifiziert, dass Pakete an entgegengesetzte Netzwerke gehende Pakete die RAS-Schnittstelle durchlaufen. Dann sollten Sie beim Anzeigen der TCP-Eigenschaften im Fehlerbehebungsprotokoll von WinRoute Administrator in der Liste der verfügbaren Schnittstellen eine DFÜ-Schnittstelle aufgeführt sehen.

3 Rufen Sie die Schnittstellentabelle in WinRoute Administration auf, und lassen Sie die Eigenschaften der RAS-Schnittstelle, die für die PPTP-Verbindung genutzt wird, anzeigen. Vergewissern Sie sich, dass Sie NAT an dieser Schnittstelle nicht ausführen.

4 Wählen Sie auf der Registerkarte "RAS" der RAS-Schnittstelleneigenschaften die PPTP-Verbindung aus den RAS-Einträgen. Falls Sie die RAS-Verbindung in den RAS-Einträgen nicht vorfinden, vergewissern Sie sich, dass Sie das richtige Telefonbuch eingerichtet haben. Öffnen Sie das Menü *Einstellungen->Erweitert->Versch. Optionen* und wählen Sie das korrekte RAS-Telefonbuch aus.

5 Überprüfen Sie die Verbindung. Sie sollten in der Lage sein, Pings an das entgegengesetzte Netzwerk zu senden und gleichzeitig auf das Internet zuzugreifen.



Ausführen von PPTP-Clients hinter NAT

Es müssen keine Einstellungen durchgeführt werden, um PPTP-Clients hinter WinRoute (NAT) auszuführen, die auf den PPTP-Server im Internet zugreifen. Sie können so viele simultane Verbindungen einrichten wie nötig.

DNS-Lösung

In diesem Abschnitt

DNS-Server auf dem WinRoute-PC

Das Ausführen eines DNS-Servers auf einem WinRoute-PC birgt keine Schwierigkeiten. Alle DNS-Anfragen, die am DNS-Server eingehen, werden mit der regulären Internet-IP-Adresse, die mit dieser Domäne assoziiert ist, beantwortet. Eine solche IP-Adresse muss mit der Schnittstelle des Netzwerks assoziiert sein, die den WinRoute-PC mit dem Internet verbindet. Die Internet-Server überwachen sowohl die öffentliche als auch die privaten Schnittstellen.

Wenn der lokale PC eine DNS-Anfrage sendet, um www.meinedomäne.com aufzulösen, erhält dieser eine öffentliche IP-Adresse mit dieser Domäne und verbindet den Web-Server mit einer IP-Adresse (die der Internetschnittstelle zugewiesen wird).

- ***Vergewissern Sie sich, dass die Anschlusszuordnung für DNS-Anfragen eingerichtet ist, auch wenn Sie den DNS-Server am WinRoute-PC ausführen! Ordnen Sie das UDP-Protokoll sowie Anschluss 53 für die IP-Adresse der Internetschnittstelle zu.***

DNS-Server hinter dem WinRoute-PC

Sie können einen DNS-Server an jedem PC innerhalb Ihres lokalen Netzwerks ausführen. Richten Sie dazu die Anschlusszuordnung wie folgt ein:

Protokoll: UDP

Überwachungs-IP: nicht spezifiziert bzw. die IP-Adresse, die mit dem DNS-Server assoziiert ist (als zweite IP-Adresse zugeordnet)

Überwachungsanschluss: 53

Ziel-IP: die private IP-Adresse des PCs mit DNS-Server

Zielanschluss: 53

DNS- und WWW-Server hinter NAT

Falls Sie Ihren eigenen DNS-Server und den WWW-Server im gleichen privaten Netzwerk ausführen, können folgende Fragen auftauchen:

Wie gehe ich mit DNS-Anfragen bezüglich www.meinedomäne.com um, die aus meinem LAN stammen. Wie werden diese mit der privaten Netzwerk- IP-Adresse des Webservers beantwortet, während DNS-Anfragen, die aus dem Internet eingehen, eine reguläre Internet-IP-Adresse mit www.meinedomäne.com erhalten?

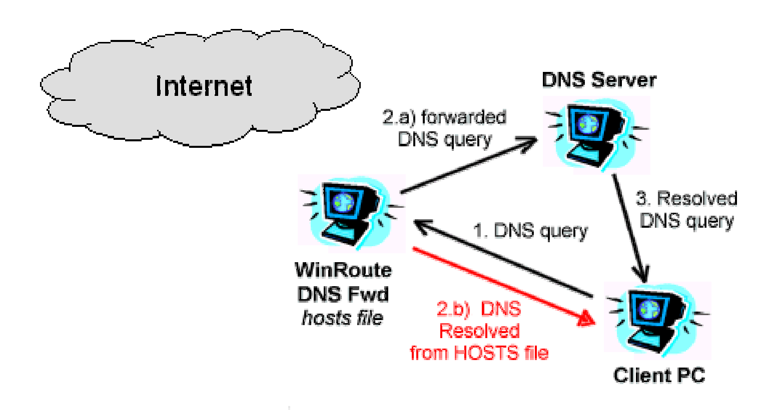
Die Antwort ist verhältnismäßig einfach. Verwenden Sie die in WinRoute integrierte **DNS-Weiterleitung**, um das Problem zu lösen. Richten Sie an allen Client-PCs die DNS-Weiterleitungsfunktion von WinRoute ein. Nehmen Sie auf dem WinRoute-PC folgende Einstellungen vor:

- Schalten Sie die DNS-Weiterleitung von WinRoute EIN.
- Bearbeiten Sie die HOSTS-Datei:

  Fügen Sie in der HOSTS-Datei eine Aufzeichnung hinzu, die besagt, dass www.meinedomäne.com eine spezielle, private IP-Adresse ist (auf der Ihr Web-Server ausgeführt wird - z. B. 10.10.10.8). Die HOSTS-Datei finden Sie im Hauptverzeichnis Ihres Windows-Verzeichnisses (in dem Windows installiert ist - c:\Windows oder c:\win98 usw.). Sie können auf die HOSTS-Datei auch über das Dialogfeld der DNS-Weiterleitung von WinRoute zugreifen, indem Sie auf die Schaltfläche zum Editieren der 'HOSTS-Datei klicken.

Wie funktioniert das?

Alle DNS-Anfragen, die von den Client-Computern Ihres LAN gesendet werden, werden zuerst von der DNS-Weiterleitung in WinRoute aufgelöst. Zunächst werden alle Anfragen mit den Datensätzen in der HOSTS-Datei verglichen. Wenn der entsprechende Datensatz auf die Anfrage zutrifft, wird diese mit den Details des Satzes (in unserem Fall die private IP-Adresse) beantwortet.



Falls keine Datensätze vorhanden sind, die der Anfrage in der HOSTS-Datei entsprechen, wird diese noch mit den Datensätzen im Cache von WinRoute (der in der DNS-Weiterleitung enthalten ist) verglichen. Wenn der DNS-Cache keinen übereinstimmenden Datensatz enthält, wird die Anfrage an den DNS-Server weitergeleitet, der in der DNS-Weiterleitung in WinRoute darauf eingerichtet ist, DNS-Anfragen zu erhalten.

Alle DNS-Anfragen, die aus dem Internet kommen, werden anhand der Einstellungen für die Anschlusszuordnung direkt an den DNS-Server weitergeleitet und den Datensätzen entsprechend aufgelöst.

- ***Hinweis! In einem solchen Fall können Sie den DNS-Server nicht auf demselben Computer wie WinRoute ausführen. Dies ist der Fall, weil beide Dienste - DNS-Forwarder (Weiterleitung) von WinRoute und Ihr DNS-Server - am gleichen Anschluss - UDP 53 - ausgeführt würden. Dies würde schwerwiegende Probleme verursachen.***

DNS

Ausführen eines Webservers (oder FTP usw.) und DNS-Servers im selben privaten Netzwerk hinter WinRoute NAT

Möglicherweise möchten Sie den Webserver mit der Domäne www.meinedomäne.com hinter NAT ausführen und Ihren DNS-Server im selben Netzwerk für die Namensauflösung verwenden.

Ausführen eines Webservers (oder FTP usw.) auf dem WinRoute-PC

Wenn Sie einen Webserver am WinRoute-PC ausführen, werden Sie mit lokalen Anfragen keine Probleme haben. Alle DNS-Anfragen für www.wasauchimmer.com, die an Ihrem DNS-Server ankommen, werden von der regulären Internet-IP-Adresse, die mit dieser Domäne assoziiert ist, verknüpft. Eine solche IP-Adresse muss der Schnittstelle des Netzwerks, die vom WinRoute-PC zum Internet und den WWW-Servern führt, zugeordnet werden, und die WWW-Server überwachen sowohl die öffentliche als auch die private Schnittstelle.

Wenn der lokale PC eine DNS-Anfrage zum Auflösen von www.wasauchimmer.com sendet, erhält dieser eine IP-Adresse, die mit dieser Domäne assoziiert ist. Dies führt dazu, dass der Webserver mit der IP-Adresse verbunden wird (die wie oben beschrieben der Schnittstelle zum Internet zugewiesen wurde).

Ausführen eines Webservers (oder FTP usw.) auf einem PC hinter WinRoute

Möglicherweise möchten Sie Ihren Webserver auf einem PC hinter WinRoute ausführen (mit einer privaten IP-Adresse z. B. 10.10.10.8). Der Webserver mit www.meinedomäne.com befindet sich physikalisch an der privaten IP-Adresse 10.10.10.8, Ihre DNS-Anfrage wird jedoch mit einer regulären IP-Adresse aufgelöst (wie 206.86.181.25), die mit dieser Domäne assoziiert wird.

Dann wendet sich Ihr Browser oder FTP-Client an die öffentliche Adresse, wo kein Server ausgeführt wird, da der Webserver sich innerhalb des Netzwerks befindet.

Lösung

Um dieses Problem zu beheben, verwenden Sie die in WinRoute integrierte **DNS-Weiterleitung (DNS- Forwarder)** als DNS-Server für Ihren Computer.

In der **HOSTS-** Datei geben Sie einen neuen Eintrag ein, der besagt, dass **www.meinedomäne.com** an der entsprechenden **internen** (privaten) IP-Adresse ausgeführt wird. Stellen Sie den DNS-Forwarder so ein, dass er die HOSTS-Datei prüft, bevor er eine DNS-Anfrage an den regulären Server sendet.

So werden immer dann, wenn Benutzer eine Anfrage an **www.meinedomäne.com** senden, solche Anfragen an die richtige lokale Adresse gesendet.

Ausführen von WWW-, FTP-, DNS- und Telnet-Servern hinter WinRoute

In diesem Abschnitt

Ausführen eines WWW-Servers hinter NAT

So führen Sie den Webserver hinter NAT aus:

1 Öffnen Sie das Menü *Einstellungen->Erweitert->Anschlusszuordnung*.

2 Fügen Sie eine neue Anschlusszuordnung hinzu:

Protokoll: TCP

Überwachungs-IP: nicht spezifiziert bzw. die IP-Adresse, die mit der Domäne assoziiert ist. Eine solche IP-Adresse muss der Schnittstelle zugeordnet sein.

Überwachungsanschluss: 80

Ziel-IP: die IP-Adresse des Webservers (z. B. 192.168.1.10)

Zielanschluss: 80

Der Zugang zu diesen Diensten erfolgt entweder über den Domänennamen oder die öffentliche IP-Adresse Ihres Netzwerks. Nachdem die Pakete WinRoute erreicht haben, werden sie automatisch an den internen Computer mit der entsprechenden internen IP-Adresse umgeleitet.

Ausführen eines DNS-Servers hinter NAT

Die in WinRoute integrierte DNS-Weiterleitung ermöglicht es, DNS-Anfragen an reguläre DNS-Server weiterzuleiten, um Domänennamen aufzulösen. Er ist in der Lage, lokale DNS-Anfragen aufzulösen (wenn der Name des lokalen Computers verwendet wird). DNS-Anfragen wie *www.wasauchimmer.com* müssen mit dem regulären DNS-Server aufgelöst werden. Die **DNS-Weiterleitungsfunktion** von WinRoute leitet DNS-Anfragen an den **DNS-Server** weiter.

Ausführend des DNS-Servers hinter NAT (WinRoute)

Um den DNS-Server hinter NAT/WinRoute auszuführen, nehmen Sie die Anschlusszuordnung wie unten beschrieben vor. Die DNS-Server kommunizieren untereinander über das **UDP-**Protokoll an **Anschluss 53**. Wenn Sie diese Einstellung nicht vornehmen, wird Ihr DNS-Server nicht funktionieren. Diese Einstellung ist obligatorisch. Wenn der DNS-Server am selben Computer wie WinRoute ausgeführt wird, führt das Inspektionsmodul von WinRoute NAT durch, **BEVOR** Pakete eine Anwendung erreichen, einschließlich des DNS-Servers.

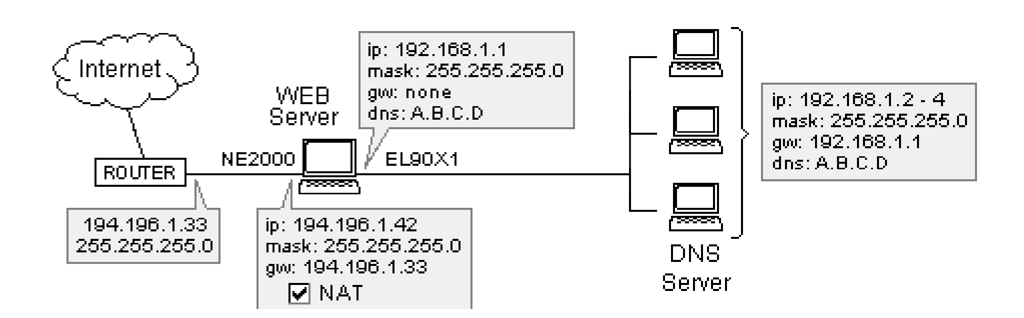
Protokoll: UDP

Überwachungs-IP: nicht spezifiziert oder die öffentliche IP-Adresse des DNS-Servers, den Sie betreiben möchten

Überwachungsanschluss: 53

Ziel-IP: öffentliche oder private IP-Adresse von DNS

Zielanschluss: 53



➢ ***Hinweis! Es ist** nicht möglich, **einen regulären DNS-Server am selben Computer wie den DNS-Forwarder von WinRoute auszuführen. Beide Dienste verwenden Protokoll UDP Anschluss 53. Beide DNS-Dienste am selben PC auszuführen, würde zu schwerwiegenden Problemen beim IP-Routing führen. Sie können jedoch die Weiterleitungsfunktion von WinRoute AUSSCHALTEN, wenn Sie den DNS-Server auf dem WinRoute-PC ausführen möchten.***

Ausführen eines FTP-Servers hinter NAT

So führen Sie einen FTP-Server hinter NAT aus:

1. Öffnen Sie das Menü *Einstellungen ->Erweitert ->Anschlusszuordnung.*
2. Fügen Sie die neue **Anschlusszuordnung** hinzu:

Protokoll: TCP

Überwachungs-IP: nicht spezifiziert oder die IP-Adresse, die mit der Domäne assoziiert ist. Eine solche IP-Adresse muss mit der Internetschnittstelle assoziiert sein.

Überwachungsanschluss: 21

Ziel-IP: Geben Sie die IP-Adresse des FTP-Servers ein (z. B.192.168.1.10)

Zielanschluss: 21

Ausführen eines FTP-Servers mit einem nicht standardmäßigen Anschluss:

Passen Sie die Anschlusszuordnung an den Anschluss an, der vom FTP-Server verwendet wird.

Ausführen des MAIL-Servers hinter NAT

Um den Mail-Server hinter WinRoute auszuführen, empfehlen wir, zwei Einträge zur Anschlusszuordnung zu erstellen - einen für das SMTP-Protokoll (wird an Anschluss 25 ausgeführt) und eines für das POP3-Protokoll (wird an Anschluss 110 ausgeführt). So können andere SMTP-Server Ihren SMTP-Server erreichen, und Sie können Ihre E-Mail über POP3 aus dem Internet abholen.

Falls der MAIL-Server auf dem WinRoute-Computer ausgeführt wird, muss die Anschlusszuordnung eingerichtet werden. Dies liegt an der Position des Inspektionsmoduls von WinRoute, das unterhalb des TCP-Stacks (Datenstapel) arbeitet, so dass die Pakete verändert/abgelehnt werden, bevor sie das Betriebssystem erreichen.

SMTP-Protokoll:

Protokoll: TCP

Überwachungs-IP:

Überwachungsanschluss: 25

Ziel-IP: IP-Adresse des SMTP-Mail-Servers (z. B. 192.168.1.10)

Zielanschluss: 25

POP3-Protokoll:

Protokoll: TCP

Überwachungs-IP:

Überwachungsanschluss: 110

Ziel-IP: IP-Adresse des POP3-Mail-Servers (z. B. 192.168.1.10)

Zielanschluss: 110

Ausführen des Telnet-Servers hinter NAT

Telnet wird von Unternehmen für die Fernverwaltung von Daten verwendet. Dieses Protokoll wird vor allem von AS400-Servern verwendet.

Um einen Telnet-Server hinter WinRoute auszuführen, ist es erforderlich, die Anschlusszuordnung für das TCP-Protokoll am Anschluss 23 einzurichten. Es ist keine Einstellung notwendig, um einen Telnet-Client auszuführen, der auf den Telnet-Server im Internet zugreift.

Protokoll: TCP

Überwachungs-IP: nicht spezifiziert oder IP des Telnet-Servers

Überwachungsanschluss: 23

Ziel-IP: IP-Adresse des Telnet-Servers (z. B. 192.168.1.10)

Zielanschluss: 23

FTP-Aspekte unter Verwendung nicht standardmäßiger Anschlüsse

In diesem Abschnitt

Zugriff auf FTP-Server mit nicht standardmäßigen Anschlüssen

Wenn Sie sich hinter WinRoute befinden und versuchen, auf einen FTP-Server mit einer anderen Anschlussnummer als 21 zuzugreifen, erhalten Sie keinen Eintrag im Verzeichnis. Damit dies funktioniert, sind folgende Schritte erforderlich:

1 Aktivieren Sie den WinRoute-Computer.

2 Schalten Sie die WinRoute-Engine aus.

3 Öffnen Sie das Menü Start->Ausführen auf dem Desktop.

4 Geben Sie "regedit" ein, um auf den Registry Editor zuzugreifen.

5 Rufen Sie HKEY_LOCAL_MACHINE/SOFTWARE/TinySoftware/WinRoute/Module/0 auf.

6 Modifizieren Sie SpecParams, so dass der Wert der Anschlussnummer des FTP-Servers entspricht, auf den Sie zugreifen möchten.

7 Schalten Sie die WinRoute-Engine wieder ein.

Jetzt sollte jeder Benutzer, der sich hinter WinRoute befindet, auf einen FTP-Server im Internet mit einem nicht standardmäßigen Anschluss zugreifen können.

➢ ***Hinweis! Sie können mehrere Anschlüsse festlegen, indem Sie zwischen den einzelnen Werten ein Leerzeichen setzen.***

FTP-Server hinter WinRoute mit einem nicht standardmäßigen Anschluss

Bei bestimmten Bedingungen (zum Beispiel bei einem Unternehmens-Client hinter einer Firewall) kann einem Benutzer eingeschränkter Zugriff auf einen FTP-Server gewährt werden, und zwar nur im **Passiv-**Modus. Falls ein FTP-Server hinter WinRoute einen nicht standardmäßigen Anschluss verwendet, kann kein Zugriff über **Passiv-**Modus eingerichtet werden. WinRoute sieht (laut Standard) Anschluss 21 als FTP an, so dass WinRoute angepasst werden muss, wenn der Benutzer einen anderen Anschluss nutzen möchte. Mit den folgenden Schritte können Sie dieses Problem beheben und den Zugang über den **Passiv-**Modus einrichten.

1 Aktivieren Sie den WinRoute-Computer.

2 Schalten Sie die WinRoute-Engine aus.

3 Öffnen Sie das Menü Start->Ausführen auf dem Desktop.

4 Geben Sie "regedit" ein, um auf den Registry Editor zuzugreifen;

5 Rufen Sie HKEY_LOCAL_MACHINE/SOFTWARE/TinySoftware/WinRoute/Mport auf. Hier finden Sie Unterordner, die den Anschlusszuordnungen entsprechende Informationen enthalten. Falls keine Unterordner vorhanden sind, gibt es keine Anschlusszuordnungen.

6. Suchen Sie anhand des vom FTP-Server verwendeten Anschlusses den Ordner mit den Anschlusszuordnungen.
7. Ändern Sie den Schlüssel *"flags"* in "1".
8. Ändern Sie den Schlüssel *"NatApp"* in "FTP".
9. Schalten Sie die WinRoute-Engine wieder ein.

Anhand dieser Einstellungen "weiß" WinRoute, dass die Pakete, die an dem von Ihnen festgelegten Anschluss eingehen, vom FTP-Protokoll stammen. Daher führt WinRoute weitere Schritte durch, um dieses komplexe Protokoll weiterzuleiten.

Spezielle Netzwerke

In diesem Abschnitt

Token-Ring-Netzwerke

Verbinden von Token-Ring-Netzwerken

Token Ring ist ein sehr spezieller Netzwerktyp. Daher gehen wir davon aus, dass nur Netzwerkexperten mit Token Ring umgehen können und halten unsere Erklärung deshalb begrenzt.

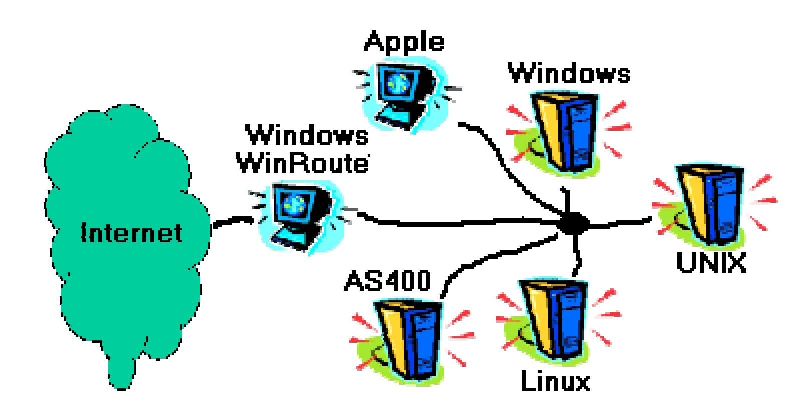
- Bei allen Computern des Token Ring muss der Wert für MTU (Maximum Transmission Unit) auf 1500 eingestellt sein.
- Öffnen Sie auf dem WinRoute-Computer das Menü *Einstellungen ->Erweitert->Versch. Optionen,* und aktivieren Sie das Kontrollkästchen für die Unterstützung von Token Ring-Netzwerken.
- Nehmen Sie andere Einstellungen vor, die für jede Art der Internetverbindung spezifisch ist.

Mehrere Betriebssysteme in einer Netzwerkumgebung (Linux, AS400, Apple)

Verbinden von Netzwerkumgebungen mit mehreren Betriebssystemen (Linux, Unix, AS400, Apple)

WinRoute eignet sich für die Internetverbindung verschiedener Netzwerkumgebungen mit unterschiedlichen Betriebssystemen. WinRoute fungiert als Software-Router und unterstützt als solcher jede standardmäßige TCP/IP-Umgebung.

- ***Hinweis! Ein auf Windows basierendes Betriebssystem dient als Host der Anwendung von WinRoute. Daher ist mindestens ein auf Windows 95/98/NT basierender Computer im WinRoute-Netzwerk erforderlich. Auf dem Host darf sich kein UNIX-System befinden, es kann jedoch als Client-System betrieben werden.***



Verbinden mehrerer Netzwerke

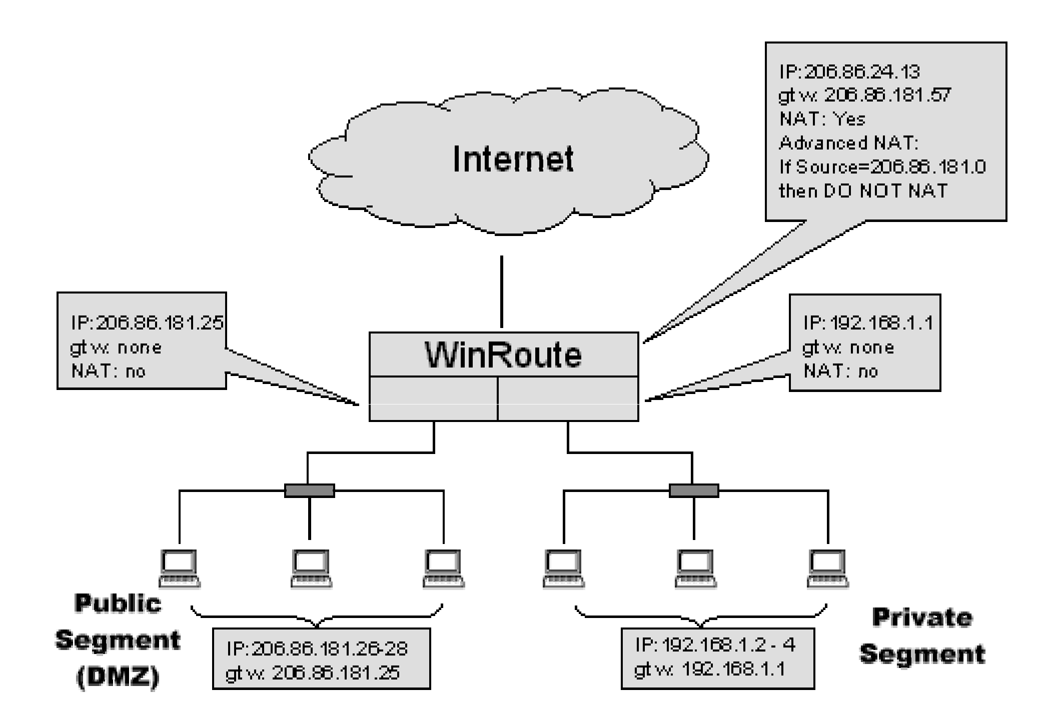
In diesem Abschnitt

Verbinden öffentlicher und privater Segmente (DMZ)

Ein privates Segment besteht aus Computern, die private Internetadressen verwenden. Solche Adressen sind privaten Netzwerken vorbehalten und können nicht im Internet verwendet werden. Daher wandelt WinRoute diese privaten Adressen in öffentliche Adressen um, so dass Sie eine Verbindung zum Internet herstellen können. Auf Computern mit einer privaten Adresse kann von außen (vom Internet) nicht direkt zugegriffen werden.

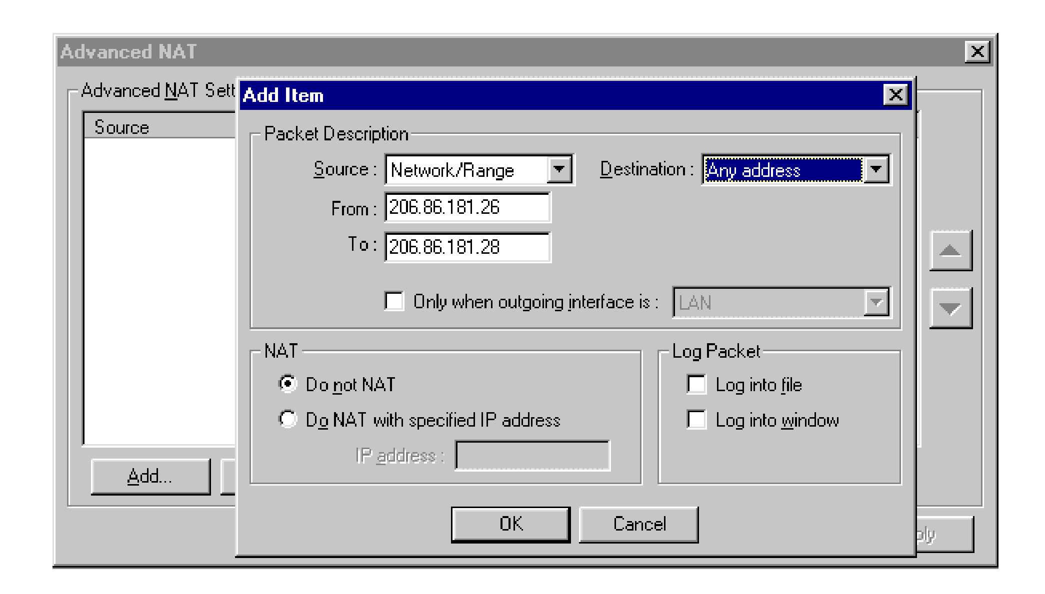
Ein öffentliches Segment besteht aus Computern, von denen jeder über eine öffentliche IP-Adresse verfügt. Auf diese Systeme kann direkt vom Internet aus zugegriffen werden, sofern die Sicherheitsregeln es zulassen.

Jedes Segment muss im WinRoute-Computer eine eigene Netzwerkschnittstelle besitzen. Dann ermöglicht es die WinRoute-Engine Ihren privaten und öffentlichen Segmenten gemeinsam eine Internetverbindung zu nutzen.



WinRoute-Einstellungen

Es ist notwendig, erweiterte NAT-Einstellungen durchzuführen, so dass WinRoute kein NAT für Pakete aus öffentlichen Segmenten durchführt. Öffnen Sie hierzu das Menü *Einstellungen=>Erweitert=>NAT*.



Einstellungen öffentlicher und privater Netzwerke

Diese Netzwerke werden auf die gleiche Art und Weise installiert, wie dies in anderen Kapiteln dieses Handbuchs beschrieben wird. Bei öffentlichen Segmenten besteht der einzige Unterschied darin, dass Sie dort öffentliche IP-Adressen verwenden. Im Wesentlichen sind folgende Regeln zu beachten:

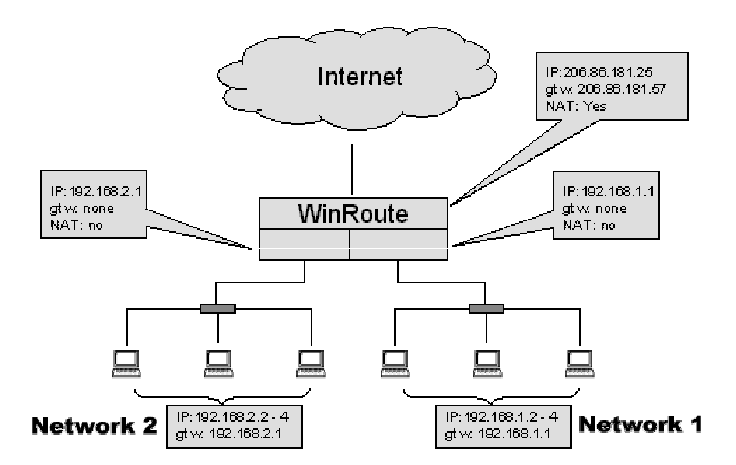
- KEIN Standard-Gateway an der Schnittstelle in WinRoute
- Die IP-Adresse dieser Schnittstelle wird als Standard-Gateway für den Rest des Netzwerks verwendet.
- KEIN NAT an den Schnittstellen in WinRoute

Weitere Erläuterungen finden Sie unter ***Checkliste*** .

Gemeinsame Nutzung der Verbindung für zwei Netzwerke mit einer IP-Adresse

Für den Fall, dass Sie zwei Netzwerke über einen Computer über WinRoute mit dem Internet verbunden haben, gibt es keine speziellen Einstellungen. Grundsätzlich gibt es mehrere Segmente, die zum WinRoute-Computer führen, von denen jeder eine separate Netzwerkschnittstelle hat. In unserem Beispiel gibt es drei Netzwerkschnittstellen im WinRoute-Computer:

- Internet-Schnittstelle
- Netzwerkschnittstelle 1
- Netzwerkschnittstelle 2



Es sind lediglich folgende Einstellungen erforderlich:

Internet-Schnittstelle

NAT ist aktiviert.
Die IP-Adresse ist gemäß den Anweisungen Ihres Internetdiensteanbieters eingerichtet.
Der Gateway ist gemäß den Anweisungen Ihres Internetdiensteanbieters eingerichtet.

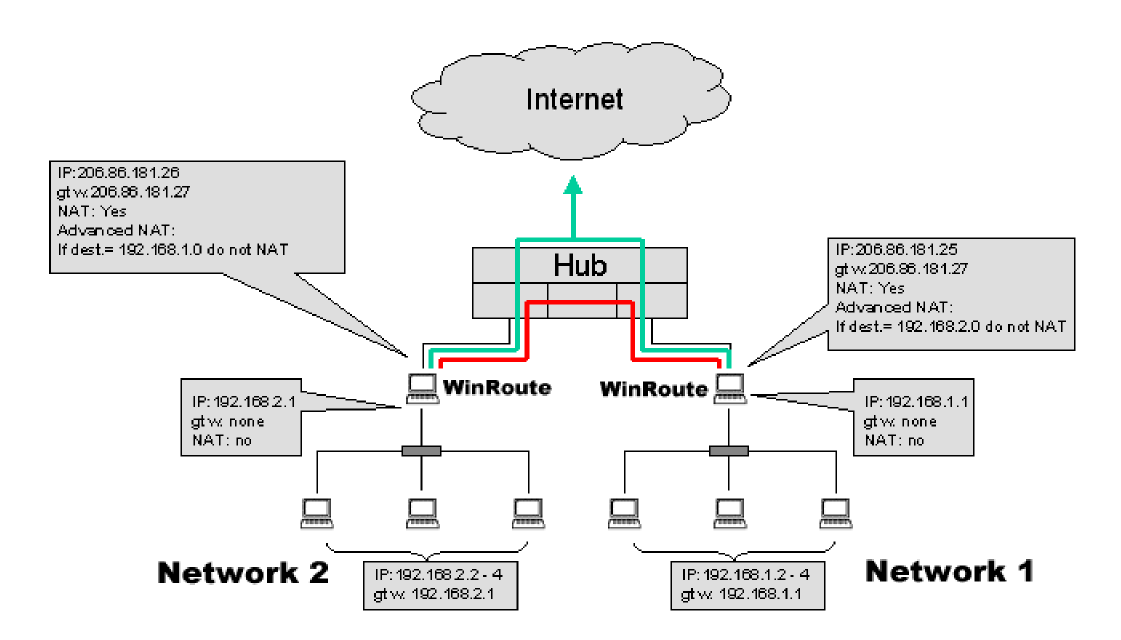
Interne Schnittstellen

NAT ist NICHT aktiviert.
Es ist an KEINER der beiden Schnittstellen ein Standard-Gateway eingerichtet.
Die IP-Adresse ist auf den internen Typ eingestellt (z. B. 192.168.1.1).

Die anderen Einstellungen sind die gleichen, wie sie in den anderen Kapiteln dieses Handbuchs beschrieben sind. Der Datenverkehr, der aus den Teilnetzen ankommt, wird in die anderen Teilnetze oder in das Internet - und umgekehrt - geleitet.

Gemeinsame Nutzung der Verbindung für zwei Netzwerke mit 2 IP-Adressen

Möglicherweise möchten Sie einen Internetzugang für zwei Netzwerke nutzen, wenn sich beide Netzwerke hinter der öffentlichen IP-Adresse befinden. Gleichzeitig soll es möglich sein, auf die Computer in beiden privaten Netzwerken zuzugreifen.



Bei der Durchführung folgender Schritte ist Folgendes DRINGEND zu beachten:

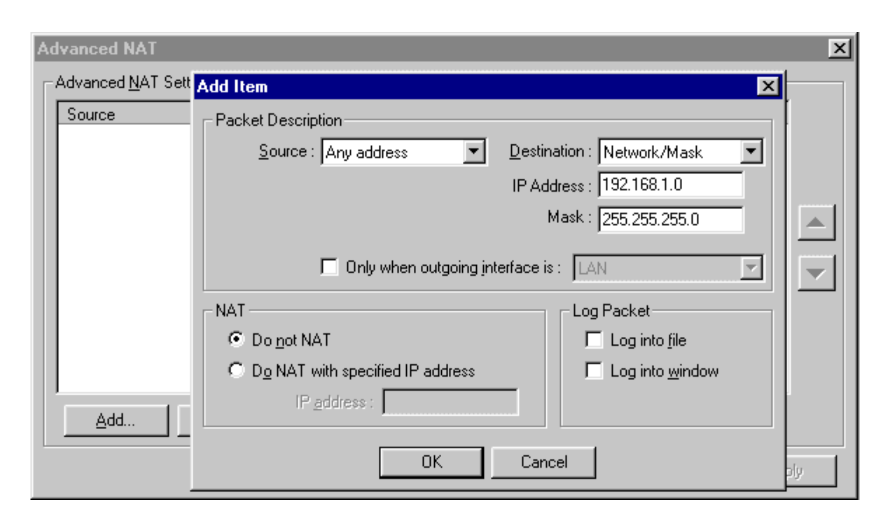
- Für alle Pakete, die in andere Netzwerke gesendet werden, KEIN NAT DURCHFÜHREN.
- Für alle an das Internet gesendete Pakete NAT DURCHFÜHREN.
- Mit anderen Worten, WinRoute führt NAT je nach Zieladresse der passierenden IP-Pakete durch. Pakete, die an das entfernte Netzwerk gehen, werden nicht verändert, während bei Paketen, die in das Internet versandt werden, NAT durchgeführt wird.

Router oder Hub?

Je nach Ihren Erfordernissen bleibt es Ihnen überlassen zu entscheiden, ob sich ein Router zwischen Ihren Netzwerken befinden soll oder ob ein Hub ausreicht. In unserem Fall gibt es einen Hub, der genügend Funktionen bietet, damit zwei Netzwerke gemeinsam eine Hochgeschwindigkeitsverbindung zum Internet nutzen können.

So richten Sie WinRoute ein, wenn für Pakete mit bestimmten Adressen keine NAT ausgeführt werden soll:

1. Öffnen Sie das Menü *Einstellungen->Erweitert->NAT*.
2. Geben Sie die Zielkriterien ein - normalerweise das Teilnetz oder der IP-Adressbereich.
3. Wählen Sie die Option "NAT nicht ausführen".



Tipp: Bei der Einstellung des erweiterten NAT werden Sie eine andere Option vorfinden, die besagt, dass NAT bei einer bestimmten IP-Quelladresse nicht durchgeführt wird. Diese Einstellung kann sinnvoll sein, wenn Sie wissen, welche Workstations nicht auf das Internet zugreifen müssen. Statt Firewall-Kriterien einzurichten, finden Sie eher eine andere Lösung in den erweiterten NAT-Einstellungen.

Wenn Sie mit speziellen Paketen keine NAT durchführen, d. h. wenn die Quelladresse weiterhin die interne IP-Adresse bliebe, werden Sie keine Antworten erhalten. Mit anderen Worten, der Benutzer würde vergeblich versuchen, eine Verbindung zum Internet herzustellen.

Server für Fernzugriff (DFÜ/Internetzugang)

Eine Server-Lösung für den Fernzugriff

Unter Umständen ist es erforderlich, dass Sie per Telefon von außen auf Ihr Unternehmensnetzwerk zugreifen und diesen Internetzugang verwenden. WinRoute bietet diese Funktion unter WindowsNT, wenn RAS-Dienste installiert und konfiguriert sind.

Bestimmte Kriterien sind einzurichten:

- Das Netzwerk Ihres Unternehmens hat ein Teilnetz (z. B. 192.168.1.0).
- Der DHCP-Server weist Benutzern, die über RAS zugreifen, IP-Adressen eines anderen Teilnetzes (z. B.192.168.2.0) zu.
- NAT wird nur an der Schnittstelle zum Internet ausgeführt.

Das bedeutet, dass die Netzwerkkarte, die zu Ihrem lokalen Netzwerk führt, die IP-Adresse eines Teilnetzes besitzen muss (z. B. 192.168.1.1). Dagegen benötigt der Benutzer, der über RAS eine Verbindung zu Ihrem Server aufbaut, eine IP-Adresse eines anderen Netzwerks (z. B. 192.168.2.1). WinRoute fungiert als Router - es kann Pakete zwischen zwei oder mehr Schnittstellen verschiedener Netzwerke umleiten, jedoch nicht aus demselben Netzwerk.

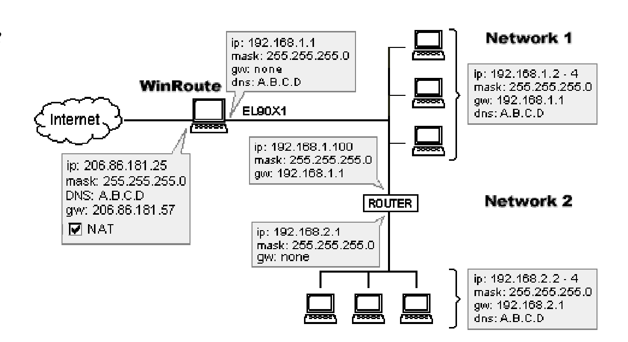
Diese Einstellung spiegelt die eines kleinen Internetdiensteanbieters wider. Mit WinRoute ist die Anzahl der Benutzer, die gleichzeitig auf Ihren NT-Server zugreifen, nicht begrenzt. Solange Ihr NT-Server IP-Adressen an externe Benutzer von verschiedenen Teilnetzen (andere als das hauptsächliche Netzwerk) ausgibt, wird die Anzahl der Benutzer durch die Anzahl der RAS-Schnittstellen, die Sie installiert haben, begrenzt.

Verbinden überlappender Segmente über eine IP-Adresse

Die Netzwerkeinstellung, bei der die zu verbindenden Netzwerke nicht direkt zum WinRoute-Computer führen und über einen Router verbunden sind, nennt man überlappende Segmente (Cascaded Segments).

Als Router zwischen den beiden Netzwerken kann jeder Hardware-Router, WindowsNT- oder Windows 95/98-Computer mit WinRoute dienen. WinRoute fungiert in jedem Fall als Router, ob er NAT ausführt oder nicht.

Figure 1: Connecting cascaded segments to the Internet



Im Allgemeinen ist es notwendig, dem WinRoute-Computer "mitzuteilen", wohin die eingehenden Pakete für andere Netzwerke gesendet werden. Dagegen muss es einen ähnlichen Link auf dem Router (der zwei Netzwerke teilt) für die ausgehenden Pakete geben, der angibt, wohin die ausgehenden Pakete aus dem zweiten Netzwerk gesendet werden. Dazu können neue Routen eingegeben werden - eine am WinRoute-Computer (für eingehende Pakete) und eine am Router (für ausgehende Pakete).

- ROUTE auf WinRoute-Computern (Mitglied von Netzwerk1) leitet IP-Pakete für das andere Netzwerk (Netzwerk2) zu dem festgelegten Netzwerk1, der IP-Adresse des Routers. Dieser Router leitet die Pakete weiter.
- DEFAULT ROUTE auf dem Router (der beide Netzwerke verbindet) leitet alle Pakete, die von Netzwerk2 kommen, an die Netzwerk1-IP-Adresse des WinRoute-Computers weiter. Dann nimmt WinRoute für diese Pakete NAT vor und sendet sie in das Internet.

Beispiel

In unserem Beispiel gibt es zwei Netzwerke 192.168.1.x und 192.168.2.x., der Router befindet sich an 192.168.1.100.

Hinweis: Als Router können Sie jeden auf Hardware basierenden Router verwenden, aber auch jeden Win95/98-Computer mit WinRoute oder Windows NT.

Einstellungen für Netzwerk1 (Hauptnetz)

- Folgendes müssen Sie Ihrem WinRoute-Computer mitteilen: " Alle Pakete, die an Netzwerk 192.168.2.0 gehen, müssen den Router 192.168.1.100 passieren":
- 1. Rufen Sie die MS-DOS-Eingabeaufforderung auf.
- 2. Geben Sie folgenden Befehl ein:

```
Route -p add 192.168.2.0 mask 255.255.255.0
192.168.1.100
```

- Auf dem Router 192.168.1.100 muss die Standardroute zum WinRoute-Computer führen, d. h. 192.168.1.1. Das bedeutet, dass Sie Ihren Router so einstellen müssen, dass alle in das Internet gehenden Pakete über den WinRoute-PC geleitet werden.
- Alle anderen Netzwerkeinstellungen werden den Erläuterungen in anderen Kapiteln entsprechend durchgeführt (Netzwerkeinstellung).

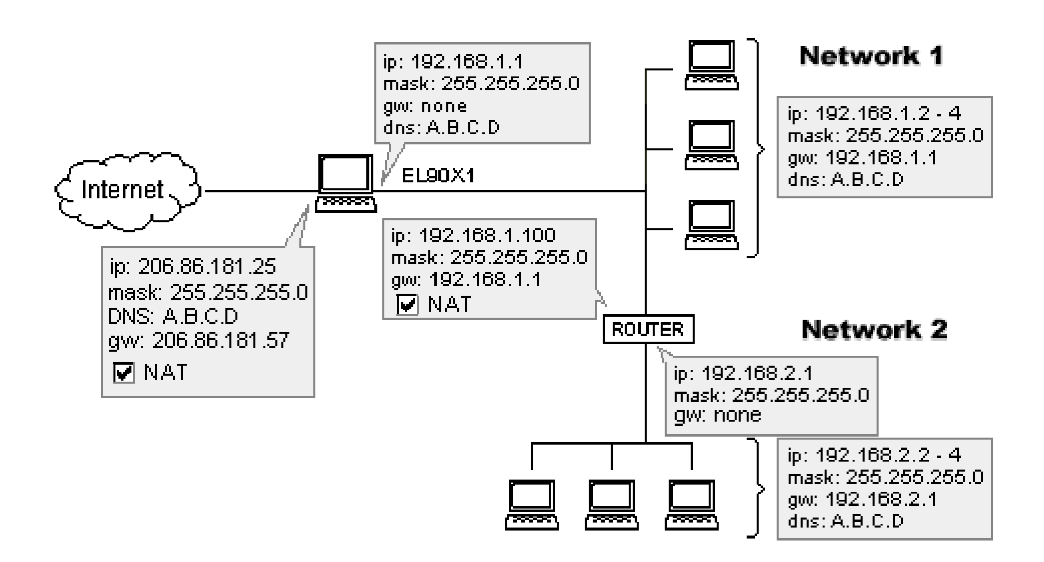
Einstellungen für Netzwerk2 (Nebennetz)

Alle Einstellungen entsprechen den regulären Einstellungen, bei denen Netzwerk2 ein eigenständiges Netzwerk darstellt. Der Standard-Gateway auf allen Computern von Netzwerk2 wird mit der IP-Adresse des Routers von Netzwerk2 eingerichtet. (In unserem Beispiel 192.168.2.1.)

NAT zwischen Netzwerk1 und Netzwerk2

Figure 2: Connecting cascaded segments to the Internet

Mit WinRoute und NAT EIN können Sie das Haupt- und Nebennetz miteinander verbinden. Das Nebennetz erscheint wie ein einzelner Computer, so dass Sie von einer einfacheren Verwaltung und erhöhter Sicherheit des Nebennetzes profitieren können. Die Einstellungen für erweiterte NAT müssen ordnungsgemäß vorgenommen werden, denn der Verkehr zwischen den beiden Netzwerken soll nicht modifiziert werden.



Einstellungen für erweitertes NAT am WinRoute-PC bei Aufteilung von Netzwerk1 und Netzwerk2

Ob NAT ausgeführt wird oder nicht, hängt von der IP-Zieladresse ab. In unserem Beispiel werden die Adressen der Pakete mit dem Zielort 192.168.1.0 nicht verändert. Auf diese Weise ist die Kommunikation zwischen diesen beiden Netzwerken möglich, so als wäre kein NAT vorhanden.

Nehmen Sie die weiteren Netzwerkeinstellungen gemäß der in diesem Handbuch beschriebenen Anweisungen vor.

Multiport-Ethernet-Adapter

Die über 170 000 Netzwerke, die derzeit WinRoute Pro als Router/Firewall-Lösung verwenden, weisen in der Regel eine Konfiguration mit zwei Netzwerkkarten auf. Die eine führt zum Internet und die andere zum lokalen Netzwerk (LAN). Diese Standardkonfiguration filtert Pakete, die in das Internet gehen oder aus dem Internet kommen. Es ist jedoch nicht möglich, Pakete, die sich zwischen lokalen Segmenten hin und her bewegen, zu filtern, da diese keinen Datenverkehr durch WinRoute leiten. Ein Beispiel für diese Konfiguration sehen Sie unten in Abbildung 1.

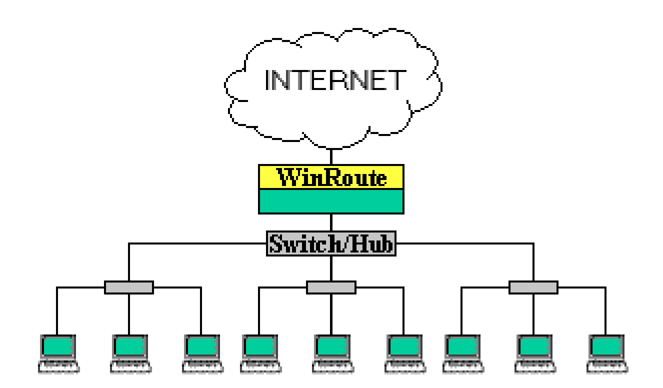


Abbildung 1. Die gängigste Konfiguration von WinRoute Pro.

In manchen Fällen kann eine dritte Netzwerkkarte für den WinRoute-PC hinzugefügt werden, welche ein separates, sicheres Segment ermöglichen. In einem solchen Fall werden Pakete, die in das sichere Segment gehen oder von dort kommen, durch WinRoute gefiltert. Damit ist eine zusätzliche Sicherheitsstufe eingebaut.

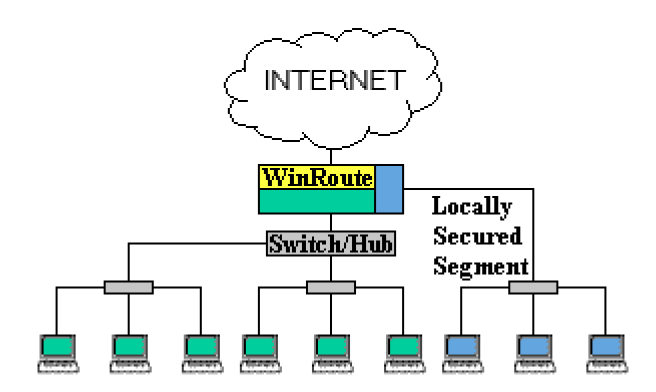


Abbildung 2. Unter Verwendung einer dritten Netzwerkkarte kann dem LAN ein separates Segment hinzugefügt werden.

Bei größeren Netzwerken, die über mehrere separate Segmente mit jeweils eigenen Sicherheitsvorkehrungen verfügen können, tritt das Problem auf, dass die Anzahl dieser separaten Segmente auf die Anzahl der Anschlüsse des WinRoute-Computers beschränkt ist. Daher ist zusätzliche Hardware notwendig, um weitere Routing- und Umschaltaktivitäten sowie Sicherheitsvorkehrungen entsprechend durchzuführen. Durch die Neueinführung von Multi-Port-Ethernet-Netzwerkkarten wurde es möglich, dass WinRoute die alleinige Kontrolle über den Netzwerkverkehr obliegt. Da der WinRoute-Computer mit Multiport-Karten bis zu 24 Anschlüsse beinhalten kann, kann der WinRoute-Computer auch als Server, Router, Switch, Domänen-Controller usw. fungieren, wobei dies von der Anzahl der Netzwerkkartensteckplätze auf der Hauptplatine abhängt. Somit kann die Verwaltung des Netzwerks zentralisiert werden und an einem einzelnen Ort kontrolliert werden. Abbildung 3 illustriert WinRoute Pro unter Verwendung einer Multiport-Ethernet-Netzwerkkarte für die Kontrolle von drei separaten Netzwerken.

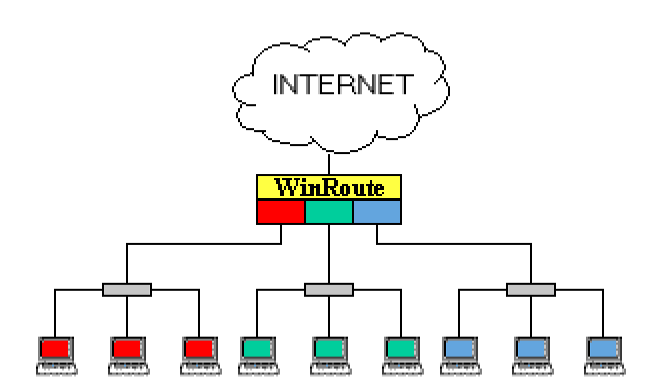


Abbildung 3. WinRoute Pro mit einer Multiport-Ethernet-Netzwerkkarte ausgestattet

Zusätzlich zur erhöhten Sicherheit und der zentralisierten Organisation bieten Multiport-Ethernet-Neztwerkkarten weitere Vorteile in Form von Lastausgleich und Ausfallschutz. Siehe die Zuweisung von drei Anschlüssen zum mittleren Segment in Abbildung 4.

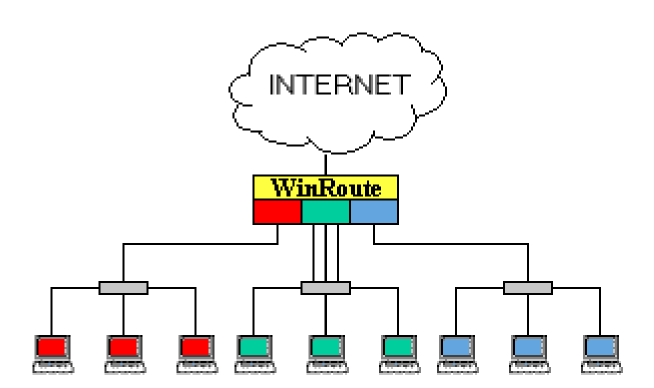


Abbildung 4. Dem mittleren Segment wurden drei Anschlüsse zur Anschlusszusammenfassung zugewiesen.

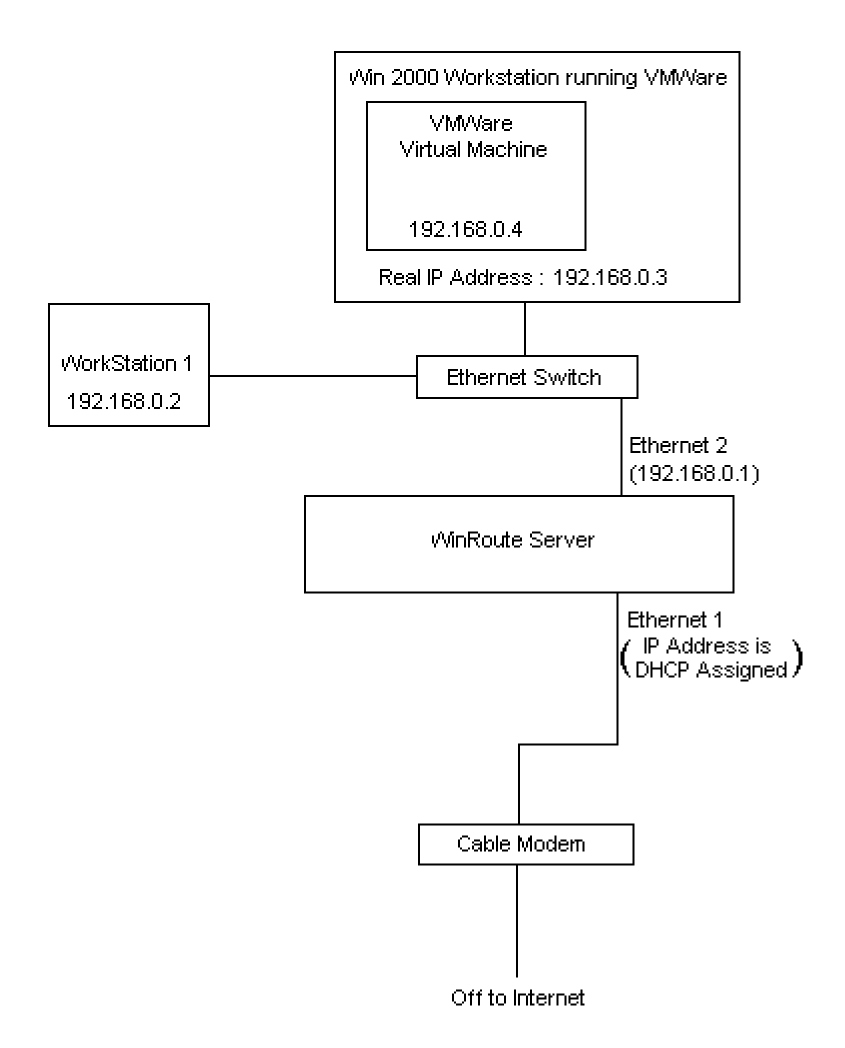
Der Lastausgleich kann durch die Zusammenfassung von Anschlüssen durchgeführt werden. In der Abbildung oben sind beispielsweise dem mittleren Segment des Netzwerks drei Anschlüsse zugewiesen. Wenn dieses Segment einen Schalter verwendet, um eine Verbindung zum WinRoute-Computer herzustellen, kann jeder der drei Computer Daten von 100 Mbps abrufen, da nur ein Anschluss dieses Segments an den WinRoute-Computer angeschlossen ist. Eine zusätzliche Funktion der Anschlusszusammenfassung (Aggregation) ist der Schutz vor einem Anschlussausfall. Wenn eine Leitung unterbrochen wird, erfolgt umgehend eine Umleitung des Datenverkehrs an den nächsten Anschluss.

Durch die Verwendung von Netzwerkkarten für mehrere Anschlüsse mit WinRoute wird ein äußerst effektives Mehrfach-Routing-System zu einem erheblich günstigeren Preis und im Rahmen einer gemeinsamen Verwaltung ermöglicht. WinRoute wurde gerade erfolgreich mit **D-Link 4 port DFE 570 TX** und **Adaptec 2 port Duralan ANA-62022** getestet. Eine andere Karte wurde nicht getestet.

Wir möchten Sie darauf hinweisen, dass diese Art des Netzwerkaufbaus unterschiedliche Teilnetze für jedes Netzwerksegment, das an den WinRoute-Computer angeschlossen ist, erfordert.

VMWare

VMWare ist eine Anwendung, die den PC, auf dem sie installiert ist, bis auf die Hardware-Ebene emulieren kann. Für das Netzwerk erscheint dieser virtuelle Computer als vollständig separate Einheit. Da der virtuelle Computer eigene Netzwerkeigenschaften aufweist, betrachtet WinRoute diesen als zusätzlichen Computer.


Win 2000 Workstation running VMWare
VMWare
Virtual Machine
192.168.0.4
Real IP Address : 192.168.0.3
WorkStation 1
192.168.0.2
Ethernet Switch
Ethernet 2
(192.168.0.1)
WinRoute Server
Ethernet 1
(IP Address is DHCP Assigned)
Cable Modem
Off to Internet

KAPITEL 4

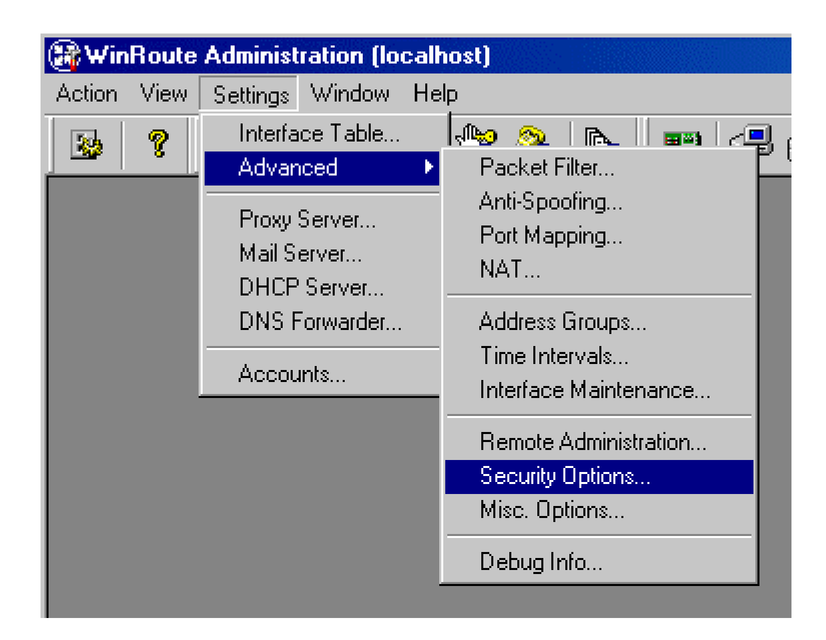
FIREWALL-KONFIGURATION

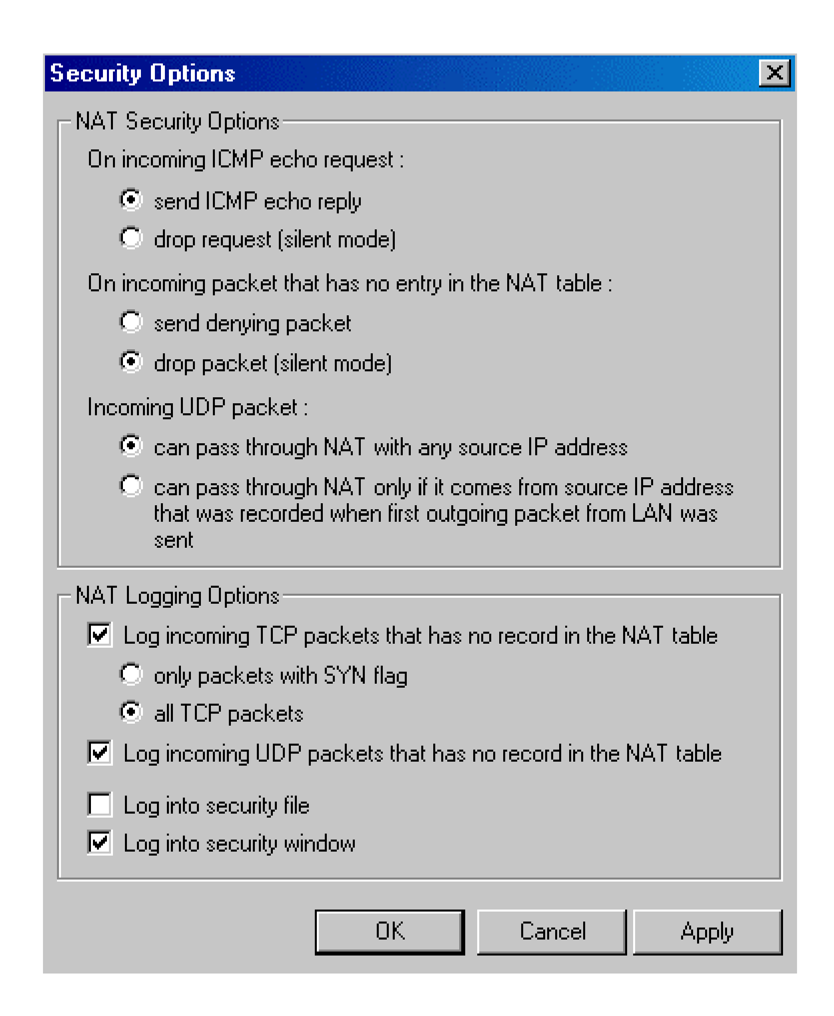
In diesem Kapitel

Korrekte Anschlusszuordnung

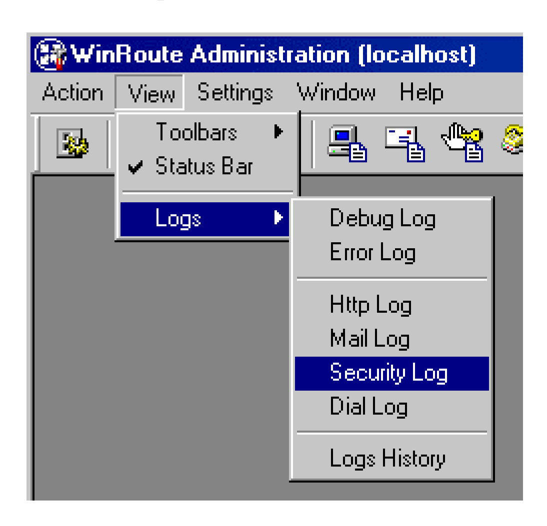
➢ ***Build 19 oder höher>***

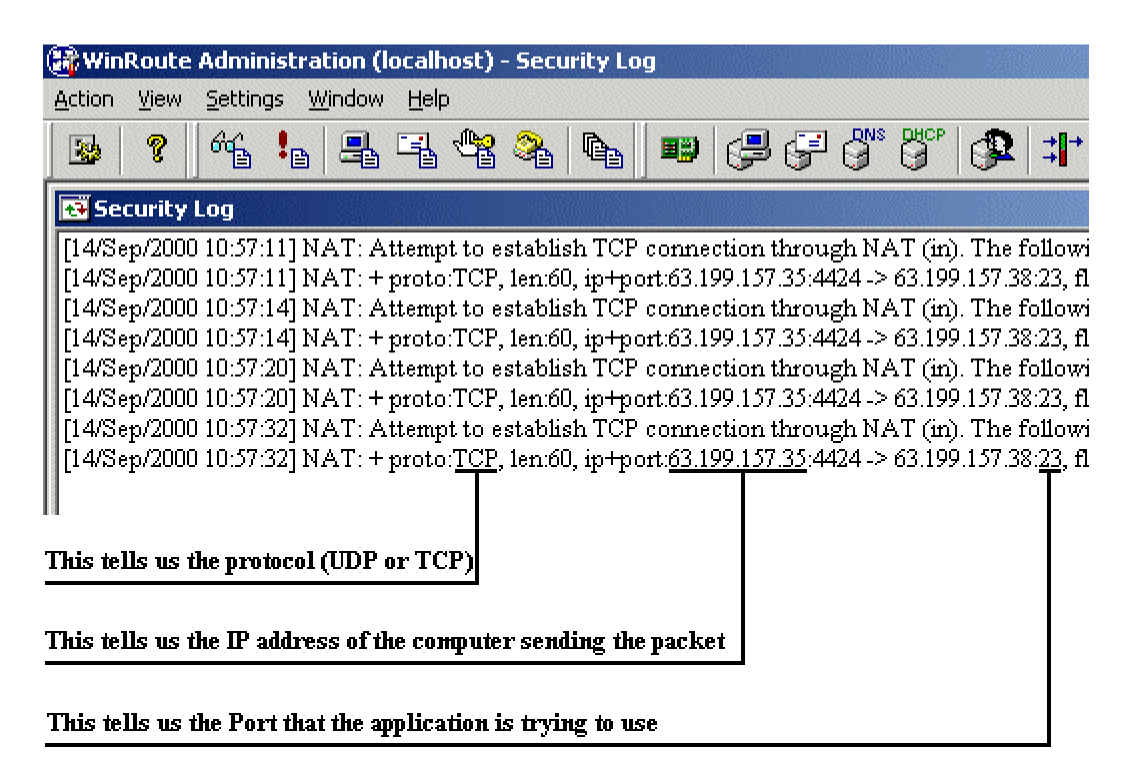
Wählen Sie im Administrations-Fenster *Einstellungen-> Erweitert-> Sicherheitsoptionen* aus.




Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

Am unteren Rand des Fensters für die Sicherheitsoptionen befinden sich einige Protokolloptionen. Aktivieren Sie die Protokollierung der TCP- und UDP-Pakete, die der NAT-Tabelle nicht bekannt sind, in das Sicherheitsfenster. WinRoute wirft diese Pakete ab, sofern keine Anschlusszuordnungen eingerichtet wurden. Da diese Protokollierungsbedingung eingeschränkt ist, wird nur eine ausgewählte Anzahl von Paketen angezeigt, um Ihnen die Suche nach der gewünschten Paketbeschreibung zu erleichtern. Öffnen Sie als nächstes das Sicherheitsprotokoll über das Menü *Ansicht-> Protokolle*.





In diesem Fall sendet ein Computer mit der Adresse 63.199.157.35 ein Paket von Anschluss 4424 zu einem Computer mit der Adresse 63.199.157.38 zu Anschluss 23. Anschluss 23 ist der Standardanschluss für Telnet. Wenn Sie einen Telnet-Server besitzen, der mit einer privaten Adresse 192.168.1.3 ausgeführt wird, erfolgt die Protokollierung an Anschluss 23. Daher würden Sie TCP-Pakete an Anschluss 23 der Adresse 192.168.1.3 zuordnen.

Kurznachrichten und Telefonie

Derzeit gibt es einige Sofortbenachrichtigungsdienste, die den Datentransfer sowie den Chat von PC zu PC oder von PC zu Telefon unterstützen. WinRoute Pro wurde mit den folgenden Konfigurationen erfolgreich getestet: **AOL Instant Messenger**, **Yahoo Instant Messenger**, **MSN Messenger** und **ICQ**.

AIM erfordert keine speziellen Einstellungen. Verwenden Sie die Standardeinstellungen für die Verbindungen, und geben Sie nicht an, dass Sie einen Proxy-Server verwenden.

Yahoo IM-Benutzer müssen die Voreinstellungen für die Anmeldung -> Verbindung in "keine Netzwerkerkennung" ändern. Alle Dienste von Yahoo IM sollten mit dieser Einstellung korrekt hinter NAT ausgeführt werden.

MSN Messenger arbeitet am besten unter Verwendung von HTTP-Proxy. Aktivieren Sie den WinRoute-Proxy am Standardanschluss 3128 (zusätzlich zur Network-Address-Translation). Der Chat von PC zu PC kann derzeit nicht ausgeführt werden, der Chat von PC zu Telefon funktioniert jedoch.

ICQ kann in den meisten Fällen mit den Standardeinstellungen der **neuesten** Version ausgeführt werden. Wenn Sie bei der Ausführung von Datenübertragungen auf Schwierigkeiten stoßen, empfehlen wir, den HTTP-Proxy, der sich in Voreinstellungen -> Verbindungen -> Server befindet, sowie die Firewall zu verwenden. Aktivieren Sie den WinRoute-Proxy am Standardanschluss 3128 (zusätzlich zur Network Adress Translation).

Hinweis: Für diese Anwendungen ist keine Anschlusszuordnung erforderlich.

H.323 - NetMeeting 3.0

WinRoute unterstützt das H.323-Protokoll. Dies bedeutet, dass alle Voice-Over-IP-Anwendungen über WinRoute kommunizieren können. Zu diesen Anwendungen gehören Microsoft NetMeeting, CuSeeMee, Telefonieren über das Internet (Sie können beispielsweise das IP-Telefon von Siemens mit WinRoute ausführen) und andere Anwendungen.

Bei Initiierung der Kommunikation hinter WinRoute

In einem solchen Fall sind keine Einstellungen erforderlich. WinRoute unterstützt eine praktisch unbegrenzte Anzahl von simultanen Verbindungen.

Einrichtung der Kommunikation vom Internet zu einem PC hinter WinRoute

In diesem Fall ist eine Anschlusszuordnung erforderlich. Das heißt, in WinRoute muss angegeben werden, wohin die eingehenden H.323-Pakete geleitet werden sollen. Nehmen Sie die Anschlusszuordnung wie folgt vor:

Protokoll:	TCP
Überwachungs-IP:	IP-Adresse, die für H.323 verwendet wird, nicht spezifiziert bei Vorliegen eines Multihome-Systems
Überwachungs-anschluss:	1720
Ziel-IP:	Die LAN-IP-Adresse der H.323-Anwendung
Zielanschluss	1720

H.323-Protokoll wird nicht nur an Anschluss 1720 ausgeführt, WinRoute fügt die anderen Verbindungen automatisch hinzu. Wegen der Begrenzung des H.323-Protokolls wird jeweils immer nur eine Workstation eine solche Datenübertragung durchführen können.

IRC - Internet Relay Chat

Für die Ausführung des IRC-Client sind keine besonderen Einstellungen erforderlich. Selbst DCC (Direkt-Chat/Send and Receive Data), eine Anwendung für direkten Chat und das Versenden bzw. Empfangen von Daten funktioniert automatisch, wenn Sie den Standardanschluss 6667 auf Ihrem IRC verwenden.

Um den IRC-Server hinter NAT auszuführen, ordnen Sie bitte die folgenden Anschlüsse zu:

Protokoll: TCP

Überwachungs-IP: nicht spezifiziert oder die IP, die Sie für Ihren IRC-Server verwenden möchten.

Überwachungsanschluss: 6667

Ziel-IP: IP-Adresse des PC mit Ihrem IRC-Server

Zielanschluss: 6667

DCC funktioniert ausschließlich mit dem Standardanschluss.

CITRIX Metaframe

WinRoute unterstützt das **CITRIX-Metaframe-**Protokoll vollständig. Führen Sie folgende Anschlusszuordnung durch, um aus dem Internet auf den CITRIX-Metaframe-Server zuzugreifen, der innerhalb des WinRoute-Netzwerks ausgeführt wird:

Für CITRIX Metaframe:

Protokoll: TCP

Überwachungs-IP: nicht spezifiziert oder die öffentliche IP-Adresse des Servers, den Sie verwenden möchten.

Überwachungsanschluss: 1494

Ziel-IP: Private IP-Adresse des Servers innerhalb des Netzwerks.

Zielanschluss: 1494

Sie können mehrere Anschlüsse einrichten und gleichzeitig auf mehrere Server zugreifen. Um dies zu tun, müssen Sie an den Client-Computern vorab einstellen, über welchen Anschluss diese auf den Server zugreifen sollen. Dies kann in der .ini-Datei des Client beim Erstellen des Verbindungssymbols festgelegt werden.

MS Terminal-Server

WinRoute unterstützt das **MS -Terminal-Server-**Protokoll vollständig. Um auf den MS-Terminal-Server innerhalb des WinRoute Netzwerks zuzugreifen, führen Sie die folgende Anschlusszuordnung durch:

Für MS-Terminal-Server:

Protokoll: TCP

Überwachungs-IP: nicht spezifiziert oder die öffentliche IP-Adresse, die der Server verwenden soll

Überwachungsanschluss: 3389

Ziel-IP: private IP-Adresse des Servers innerhalb des Netzwerks

Zielanschluss: 3389

Sie können mehrere Anschlüsse einrichten und gleichzeitig auf mehrere Server zugreifen. Um dies zu tun, müssen Sie an den Client-Computern vorab einstellen, über welchen Anschluss diese auf den Server zugreifen. Dies kann beim Erstellen des Verbindungssymbols in der .ini-Datei des Client festgelegt werden.

Internettelefonie - BuddyPhone

WinRoute ist die erste Router/Firewall-Software auf dem Markt, die der Geschäftswelt das Telefonieren über das Internet auf hohem Niveau ermöglicht. BuddyPhone ermöglicht es Ihnen, einen Anruf über das Internet von einem Netzwerk zu einem anderen zu tätigen.

Am besten wird BuddyPhone von ICQ unterstützt. Registrieren Sie sich für diese Instant-Messenger-Software und telefonieren Sie mit Ihren Freunden per Mausklick.

Alle Benutzer, die in Ihrer Buddy-Liste aktiviert sind, erscheinen in Ihrem BuddyPhone-Telefonbuch, und für einen Anruf ist nichts weiter erforderlich, als den gewünschten Benutzer aus der Liste auszuwählen.

Wenn Sie BuddyPhone und ICQ zusammen verwenden, sind keine Einstellungen erforderlich.

Die Verwendung von BuddyPhone ohne ICQ

WinRoute kann Anrufe, die aus dem Internet kommen, anhand des Anschlusses an den richtigen Empfänger im lokalen Netzwerk weiterleiten.

Um den lokalen Benutzern eigene Anschlüsse zuzuordnen, verwenden Sie die Anschlüsse 710 und höher.

Beispiel:

Innerhalb Ihres LAN verwenden drei Benutzer BuddyPhone.

Benutzername	Benutzer-IP, interne IP-Adresse	Dem Benutzer zugeordneter Anschluss
Johann	192.168.1.2	710

Guido	192.168.1.3	711
Robert	192.168.1.4	712

Dann führen Sie eine Anschlusszuordnung durch:

Überwachungsanschluss	Ziel-IP	Zielanschluss
710	192.168.1.2	700
711	192.168.1.3	700
712	192.168.1.4	700

Das Telefongespräch mit einem Benutzer ist so einfach sein wie die Eingabe von Unternehmen.com:port# im Direktwahl-Dialog von BuddyPhone. Zum Beispiel: sales.gamerouter.com:711.

➢ ***Hinweis! Hierbei handelt es sich nicht um einen Fehler in unserer Dokumentation! Der Zielanschluss ist wirklich 700. Dies ist die Anschlussnummer, die von BuddyPhone zur Ausführung verwendet wird. WinRoute führt die Weiterleitung basierend auf dem Überwachungsanschluss durch.***

CU-YouSeeMe

Um über NAT (hinweg) **CU-SeeMe-**Anrufe zu erhalten, sind die folgenden Anschlusszuordnungen erforderlich:

Protokoll: UDP

Überwachungs-IP: <nicht spezifiziert>

Überwachungsanschluss: 7648

Ziel-IP: IP-Adresse des Computers, der den CU-SeeMe-Client ausführt.

Zielanschluss: 7648

Protokoll: UDP

Überwachungs-IP: <nicht spezifiziert>

Überwachungsanschluss: 7649

Ziel-IP: IP-Adresse des Computers, der den Cu-SeeMe-Client ausführt.

Zielanschluss: 7649

Einschränkungen:

- Derzeit ist es nicht möglich, mehr als einen CU-SeeMe-Client in einem lokalen Netzwerk auszuführen.
- Es ist nicht möglich, eine Verbindung zu einem "Reflektor" herzustellen, der durch ein Kennwort geschützt wird.

Fernzugriff - PC Anywhere

In diesem Abschnitt

PC Anywhere

Von allen auf dem Markt erhältlichen Router-Programmen bietet WinRoute eine einzigartige Unterstützung für PC Anywhere von Symantec. PC AnyWhere ermöglicht es dem Benutzer, innerhalb eines Netzwerks auf Computer zuzugreifen und diese zu verwalten. Nehmen Sie hierzu folgende Schritte vor:

1. Der verwaltete Computer führt den Host von PC Anywhere aus.
2. Der Fern-Computer führt PC Anywhere Remote aus.
3. Die Anschlusszuordnung am WinRoute-Computer wird folgendermaßen konfiguriert:

   Protokoll: TCP/UDP

   Überwachungs-IP: nicht spezifiziert

   Überwachungsanschluss (Bandbreite): 5631-5632

   Ziel-IP: IP-Addresse des Host von PC-Anywhere innerhalb Ihres Netzwerks (z. B. 192.168.1.12)

   Zielanschluss: 5631-5632

Sicherheit

Um die Sicherheit zu erhöhen und Ihr Netzwerk für die Außenwelt unzugänglich zu machen, können Benutzer eine bestimmte IP-Adresse auswählen, von der aus der Zugang über festgelegte Anschlüsse erlaubt ist. Mit dieser Konfiguration können nur bestimmte Computer oder Netzwerke, auf Ihr System vom Internet aus zuzugreifen.

Um Computer zu installieren, denen der Zugriff auf Ihr Netzwerk gewährt sein soll, legen Sie zuerst eine Adressengruppe fest (auch wenn Sie nur einen einzelnen Computer eingeben). Um diese Konfiguration zu erstellen, rufen Sie das Menü *Einstellungen=>Erweitert=>Adressengruppen* auf.

Verändern des Zugriffs auf verschiedene Computer

Die Verwaltungsrechte in WinRoute lassen sich so einrichten, dass eine direkte Verbindung zum WinRoute-Host aktiviert wird. Während Sie sich in WinRoute befinden, können Sie die Ziel-IP in der Anschlusszuordnung verändern und sogar direkt auf den von Ihnen gewählten PC zugreifen.

PC Anywhere-Gateway

Wenn PC Anywhere im Gateway-Modus an der Firewall von WinRoute ausgeführt wird, kann der entfernte Client eine Liste der verfügbaren Hosts von PC Anywhere, die hinter der Firewall ausgeführt werden, abrufen. Mit Hilfe dieser Liste können Sie alle Hosts von PC Anywhere hinter der Firewall von WinRoute verwalten.

Die folgenden Anweisungen setzen voraus, dass Sie PC Anywhere 9.0 verwenden und eingehende beziehungsweise ausgehende Pakete an der Firewall von WinRoute nicht filtern.

- Die verwalteten Computer hinter der Firewall von WinRoute führen den Host von PC Anywhere unter Verwendung von TCP/IP aus.
- Der Fern-Computer führt Remote von PC Anywhere unter Verwendung von TCP/IP aus.

- PC Anywhere ist an der Firewall von WinRoute installiert und verwendet den Gateway-Modus. Bei der Konfiguration des Gateway-Computers sollten die Computer für den Dateneingang sowie den Datenausgang auf TCP/IP eingestellt sein.
- An der WinRoute Firewall muss PC Anywhere so konfiguriert sein, dass es die interne Netzwerkkarte überwacht (z. B. 192.168.1.1). Nähere Informationen zur Konfiguration von PC Anywhere, um einer bestimmte IP-Adresse/eine bestimmte Netzwerkkarte zu überwachen, finden Sie auf der Webseite von Symantec.
- Fügen Sie die genaue(n) IP-Adresse(n) der zu verwaltenden Computer in den Netzwerk-Optionen von PC Anywhere hinzu. Um das gesamte Teilnetz zu überwachen, verwenden Sie 255 für das letzte Oktett (192.168.1.255).
- Konfigurieren Sie die Anschlusszuordnung in WinRoute folgendermaßen:

  Protokoll: TCP/UDP

  Überwachungs-IP: Externe Netzwerkkarte (206.86.181.25)

  Überwachungsanschluss: BEREICH (5631-5632)

  Ziel-IP: Interne Netzwerkkarte (192.168.1.1)

  Zielanschluss: 5631-5632

Spiele

In diesem Abschnitt

Informationen zur Ausführung von Spielen hinter NAT

Spiele

Heute unterstützen viele Spiele eine Mehrbenutzerumgebungen. Die Benutzer können sich über das Internet oder das LAN bekämpfen oder gemeinsam einen der Spiele-Server im Internet nutzen. Außderdem haben sie die Möglichkeit einen eigenen Spiele-Server auf Ihrem Host einzurichten und können somit Freunde, der Familie oder völlig fremde Personen an den Spieleabenteuern teilhaben lassen.

Es gibt viele Spiele, die keine zusätzlichen Einstellungen in WinRoute erfordern. Bevor Sie versuchen, WinRoute für ein bestimmtes Spiel zu konfigurieren, verwenden Sie zunächst die Demoversion dieses Spiels. Im Gegensatz zu Proxy-Servern unterstützt die allgemeine Architektur von WinRoute viele Spiele, ohne dass zusätzliche Konfigurationseinstellungen erforderlich sind.

Einige Spiele erfordern für deren Ausführung jedoch die Konfiguration eines speziellen Anschlusses in WinRoute. Die Anschlüsse dienen im Allgemeinen der weiteren Identifizierung des Spielers auf dem Spiele-Server.

Falls das Spiel mit einem bestimmten Anschluss verbunden ist, stellt dies für WinRoute absolut kein Problem dar! Konfigurieren Sie einfach die Anschlusszuordnung in WinRoute so, dass im Netzwerk ankommende Pakete an den Computer des Spielers hinter der Firewall weitergeleitet werden.

Die verwendeten Anschlüsse variieren von Spiel zu Spiel. Bitte lesen Sie in der Dokumentation zu dem jeweiligen Spiel nach, oder rufen Sie den technischen Support Ihres Händlers an, um ausführlichere Informationen zu erhalten. Dieses Handbuch enthält nur einige Beipiele zu den Einstellungen der bekanntesten Spiele.

Aasheron's Call

Asheron's Call ist ein bekanntes Spiel der Microsoft Gaming Zone. Folgende Einstellungen sind für die Ausführung dieses Spiels auf einem Computer hinter GameRouter erforderlich:

1 Öffnen Sie das Menü *Einstellungen->Erweitert->Anschlusszuordnung.*

2 Nehmen Sie folgende Einstellungen vor:

Name:	S1	S2	S3	S4	S5
Anschluss-nummer:	2300-2400	9000-9013	6667	28800 - 29000	
Ziel-IP:	IP des PC mit dem Spiel	IP des PC mit dem Spiel	IP des PC mit dem Spiel	IP des PC mit dem Spiel	IP des PC mit dem Spiel
Protokoll:	TCP/UDP	UDP	TCP	TCP	

Battle.net (Blizzard)

Folgende Anschlusszuordnung ist für die Spiele von Battle.net erforderlich. Es kann jeweils nur ein Spieler teilnehmen.

Protokoll: TCP/UDP

Überwachungs-IP: nicht spezifiziert

Überwachungsanschluss: 6112

Ziel-IP: IP-Adresse des Spieler-Computers (z. B.192.168.1.6)

Zielanschluss: 6112

Half-Life

Half-Life

Protokoll: TCP/UDP

Überwachungs-IP: nicht spezifiziert

Überwachungsanschluss: 27015

Ziel-IP: IP-Adresse des Spieler-Computers (z. B. 192.168.1.6)

Zielanschluss: 27015

MSN Gaming Zone

Folgende Konfiguration wurde mit MechWarior3 in der **MSN Gaming Zone** gründlich getestet. Es kann nur jeweils ein Computer auf MSN zugreifen.

1. Öffnen Sie das Menü *Einstellungen->Anschlusszuordnung.*
2. Fügen Sie eine neue Anschlusszuordnung hinzu.

   Protokoll: TCP

   Überwachungs-IP: "nicht spezifiziert"

   Überwachungsanschluss: Bandbreite 2300 bis 2400

   Ziel-IP: die lokale IP-Adresse des Computers, den Sie mit MSN verbinden möchten

   Zielanschluss: Bandbreite 2300 bis 2400
3. Fügen Sie eine weitere Anschlusszuordnung hinzu.

   Protokoll: UDP

   Überwachungs-IP: "nicht spezifiziert"

   Überwachungsanschluss: Bandbreite 28800 bis 28912

Ziel-IP: die lokale IP-Adresse des Computers, den Sie mit MSN verbinden möchten.

Zielanschluss: Bandbreite 28800 bis 28912

Quake

Quake 3

Quake 2/3-Clients

Es sind keine speziellen Einstellungen erforderlich.

Quake 2/3-Server

Für Master-Server:

Protokolll: UDP

Überwachungs-IP: nicht spezifiziert

Überwachungsanschluss: Einfach-8002

Ziel-IP: x.x.x.x

Zielanschluss: 8002

Für Clients, die mit dem Arena-Server von Quake3 verbunden sind:

Protokoll: UDP

Überwachungs-IP: nicht spezifiziert

Überwachungsanschluss: Einfach-27960

Ziel-IP: x.x.x.x

Zielanschluss: 27960

StarCraft

StarCraft

WinRoute Pro beinhaltet eine einzigartige Unterstützung für alle StarCraft-Spieler (Blizzard Entertainment). Mehrere Spieler des Netzwerks, die über WinRoute Pro mit dem Internet verbunden sind, können gegen ihre virtuellen "Feinde" im Internet zu spielen.

Derzeit besteht eine vollständig automatische Unterstützung, nur für den Fall, dass alle Spieler eines Netzwerks, die an dem Spiel über Computer teilnehmen, die sich hinter WinRoute Pro befinden und nicht auf dem Host-Rechner.

Weitere Einzelheiten hierzu finden Sie unter www.tinysoftware.com.

Zusätzliche Anschlusszuordnungen für gängige Spiele und Anwendungen

Für verschiedene Anwendungen erforderliche Anschlüsse

Age of Empires II - 2 Anschlusszuordnungen erforderlich

Protokoll: TCP

Quell-IP: nicht spezifiziert

Quellanschluss: 47624

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: 47624

Protokoll: TCP/UDP

Quell-IP: nicht spezifiziert

Quellanschluss: Bandbreite 2300 - 2400

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: Bandbreite 2300 - 2400

Delta Force

Protokoll: TCP

Quell-IP: nicht spezifiziert

Quellanschluss: Bandbreite 3568 - 3569

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: Bandbreite 3568 - 3569

Dial Pad

Protokoll: UDP

Quell-IP: nicht spezifiziert

Quellanschluss: Bandbreite 51200 - 51201

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt.

Zielanschluss: Bandbreite 51200 - 51201

Gamespy

Registrierung

Protokoll: UDP

Quell-IP: nicht spezifiziert

Quellanschluss: 25635

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt.

Zielanschluss: 25665

Für die Spiele an sich:

Protokoll: UDP

Quell-IP: nicht spezifiziert

Quellanschluss: Bandbreite 25000 - 30000

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt.

Zielanschluss: Bandbreite 25000 - 30000

Kali - 3 Anschlusszuordnungen erforderlich

Protokoll: UDP

Quell-IP: nicht spezifiziert

Quellanschluss: 2213

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: 2213

Protokoll: UDP

Quell-IP:nicht spezifiziert

Quellanschluss: 6666

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: 6666

Protokolll: UDP

Quell-IP: nicht spezifiziert

Quellanschluss: 57

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: 57

Mplayer

Protokoll: TCP/UDP

Quell-IP: nicht spezifiziert

Quellanschluss: 8000 - 9000

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: 8000 - 9000

Für PC Anywhere Versionen 2.0 - 7.51 - 2 Anschlusszuordungen erforderlich

Protokoll: TCP

Quell-IP: nicht spezifiziert

Quellanschluss: 65301

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: 65301

Protokoll: UDP

Quell-IP: nicht spezifiziert

Quellanschluss: 22

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: 22

Quicktime - 2 Anschlusszuordnungen erforderlich

Protokoll: TCP

Quell-IP: nicht spezifiziert

Quellanschluss: 554

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: 554

Protokoll: UDP

Quell-IP: nicht spezifiziert

Quellanschluss: Bandbreite 6970 - 6999

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: Bandbreite 6970 - 6999

RTSP

Protokoll: UDP

Quell-IP: nicht spezifiziert

Quellanschluss: Bandbreite 6970 - 7170

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: Bandbreite 6970 - 7170

VNC

Protokoll: TCP

Quell-IP: nicht spezifiziert

Quellanschluss: 59xx (abhängig von der Display-Nummer)

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: 59xx

Protokoll: TCP

Quell-IP: nicht spezifiziert

Quellanschluss: 58xx

Ziel-IP: IP-Adresse des Computer, der die Anwendung ausführt

Zielanschluss: 58xx

GLOSSAR DER TERMINOLOGIE

A

Anschluss

Ein Anschluss ist eine 16-Bit-Nummer (mit einer zulässigen Bandbreite von 1 bis 65535), die von den Protokollen der Transportebene verwendet wird - dem TCP- und dem UDP-Protokoll. Anschlüsse werden verwendet, um die auf einem Computer ausgeführten Anwendungen (Dienste) zu adressieren. Wenn nur eine einzige Netzwerk-Anwendung auf dem Computer ausgeführt wird, sind keine Anschlussnummern erforderlich und die IP-Adresse allein reicht aus, um Dienste abzurufen.

Einige Anwendungen können jedoch gleichzeitig an einem bestimmten Computer ausgeführt werden und müssen daher unterschieden werden. Für diesen Zweck gibt es die Anschlussnummern. Eine Anschlussnummer kann somit als Adresse einer Anwendung innerhalb des Computers betrachtet werden.

Anschlusszuordnung

Die Anschlusszuordnung (oder Port Address Translation - PAT) ist der Vorgang, bei dem die an der Schnittstelle ankommenden Pakete in Bezug auf Anschlussnummer und IP-Adresse, die sie erreichen sollen, überprüft werden. Mit Hilfe der Anschlussnummern macht eine IP-Adresse diese Pakete ausfindig, die an die im Voraus festgelegte private IP-Adresse des lokalen Netzwerks weitergeleitet werden.

ARP

Address Resolution Protocol assoziiert eine IP-Adresse mit einer Hardware-Adresse, indem der sendende Computer aufgefordert wird, zusätzliche Daten - genannt MAC-Adresse - bereitzustellen. WinRoute verwendet ARP nur zu Protokollzwecken, um die Sicherheit zu erhöhen.

B

BOOTP

Bootstrap Protocol bezieht sich auf die Computer innerhalb eines lokalen Netzwerks, die so eingestellt sind, dass sie eine ihnen dynamisch vom DHCP-Server zugewiesene IP-Adresse akzeptieren.

C

Cache

Bezeichnet den Platz, an dem Daten zeitweise gespeichert werden. WinRoute verwendet den Cache (Zwischenspeicher) zur temporären Speicherung von Internetseiten, um die Bandbreite zu erhalten.

D

DHCP

Dynamic Host Configuration-Protokoll ist ein Protokoll, das die Verwaltung von IP-Adressen für lokale Computer organisiert und vereinfacht. In vielen Fällen (so wie bei Verwendung von WinRoute) wird zur weiteren Vereinfachung ein DNS-Server in den DHCP-Server integriert. Durch die Angabe der IP-Adresse eines besonderen Netzwerkcomputers - normalerweise handelt es sich dabei um den Computer mit Internetverbindung - verwendet DHCP die DNS-Werte des Computers.

DNS

Domain Name System ist ein Benennungsschema für die Zuweisung von IP-Adressen. www.tinysoftware.com ist beispielsweise ein Domänenname und verfügt über eine damit verbundene IP-Adresse. DNS wird verwendet, da es einfacher ist, sich einen Domänennamen zu merken als eine Zahlenfolge.

E

ETRN

ETRN ist ein vom SMTP-Server verwendeter Befehl, um eine Zeitverlängerung herzustellen/zu vereinbaren. Nachdem der SMTP-Server eine Verbindung hergestellt hat, sollte dieser eine Anfrage für SMTP-Mail ausführen.

Der ETRN-Befehl wird überall dort verwendet, wo ein SMTP-Server nicht 24 Stunden "online" ist und die E-Mails für solche Server in einem Zwischenspeicher eines anderen SMTP-Servers gespeichert werden müssen.

F

Firewall

Firewall ist ein Filtermodul, das sich an einem Gateway-Computer befindet, der den gesamten eingehenden und ausgehenden Datenverkehr überwacht, um festzustellen, ob dieser an seinen Bestimmungsort geleitet werden darf. WinRoute bietet eine erweiterte Firewall-Funktionen durch: NAT-Dienste, die Zuweisung von Richtlinien für festgelegte IP-Adressen und die Fähigkeit, den Versand bestimmter Daten zu protokollieren, so dass sie auf dem Rückweg wieder autorisiert werden können.

Flags

Flags (Merker) sind der Teil des Paketes, der zusätzliche Daten enthält, die von Routern verwendet werden. Nachstehend sind die von WinRoute angezeigten Flags aufgelistet:

SYNC - Synchronize (Synchronisieren) - das eine TCP-Verbindung herstellende Paket

ACK - Acknowledge (Bestätigen) - Bestätigung des Datenaustauschs

RST - Reset (Zurücksetzen) - Anfrage zur Wiederherstellung der Verbindung

URG - Urgent (Dringend) - dringendes Paket

PSH - Push - Anfrage zur sofortigen Weiterleitung des Pakets an in höhere Ebenen

FIN - Finalize (Abschließen) - Verbindungsaufbau abschließen

FTP

File Transfer Protocol ist ein Anwendungsprotokoll, mit dem Daten über das Internet übertragen, aktualisiert, gelöscht, verschoben, umbenannt oder kopiert werden.

G

Gateway

Eingangsstelle von einem Netzwerk in ein anderes. Ein Gateway ist für die ordnungsgemäße Verteilung der Daten zuständig, die in ein lokales Netzwerk eingehen oder aus diesem versandt werden. Auf dem Gateway-Computer, der auch als Host-Computer bezeichnet wird, muss WinRoute installiert sein.

I

ICMP

Internet Control Message Protocol verwendet Datagramme, um Fehler in der Datenübertragung zwischen Host und Gateway aufzuzeichnen.

IP-Adresse

Die IP-Adresse ist die individuelle 32-Bit-Nummer, die den Computer innerhalb eines IP-Netzwerks identifiziert. Jedem Computer im Internet wird eine eindeutige IP-Adresse zugewiesen. Die Informationen darüber, von welcher Adresse aus das Paket gesendet wurde (IP-Quelladresse) und an welche Adresse es geliefert werden soll (IP-Zieladresse), ist in jedem Paket in das bzw. vom Internet, enthalten.

IPSEC

Internet Protocol Security ermöglicht die Autorisierung und Verschlüsselung virtueller Privatnetze des Senders. WinRoute unterstützt die Novel und Cisco-Varianten der IPSEC.

L

LAN

Ein Local Area Network (LAN), ein lokales Netzwerk, ist eine Gruppe von miteinander verbundenen Computern, die Ressourcen gemeinsam nutzen können.

M

MAC-Adresse

Die Media-Access-Control-Adresse ist eindeutiger als die IP-Adresse und kann nicht verändert werden, da diese jede Hardware-Komponente eines Netzwerks spezifiziert.

MX-Records

MX-Records beinhalten Daten bezüglich anderer MAIL-Server im Internet. Durch die Verwendung von MX-Records können Sie Ihren Internetdiensteanbieter umgehen und E-Mails direkt an den gewünschten Mail-Server senden.

Dies ist von Vorteil, wenn der MAIL-Server Ihres Diensteanbieters *nicht zuverlässig* ist. Auf der anderen Seite der *direkte Versand an den Zielort* ein Einfluss auf die Dauer dieses E-Mail-Versands haben. Für den Fall, dass der *Ziel-Mail-Server* nicht erreichbar ist, verbleibt die E-Mail in der Warteschlange der ausgehenden E-Mails als *nicht gesendet* auf Ihrem Mail-Server von WinRoute.

N

NAT

Mit NAT - Network Address Translation - können Sie das Netzwerk über eine einzige IP-Adresse mit dem Internet verbinden. Die Computer innerhalb des Netzwerks nutzen das Internet so, als wenn sie direkt mit dem Internet verbunden wären (mit gewissen Einschränkungen).

Die Verbindung eines gesamten Netzwerks, das eine einzige registrierte IP-Adresse verwendet, wurde möglich, da das NAT-Modul die Quelladresse der von den lokalen Computer versandten Pakete mit der Adresse des Computers, auf dem WinRoute ausgeführt wird, ersetzt.

NAT unterscheidet sich deutlich von verschiedenen Proxy-Servern und Gateways auf Anwendungsebene, die niemals so viele Protokolle wie NAT unterstützen können.

Netzwerkmaske

Die Netzwerk-Maske wird verwendet, um IP-Adressen in Gruppen zusammenzufassen. Jedem Netzwerksegment wird eine Gruppe von Adressen zugewiesen. Die Maske 255.255.255.0 umfasst 254 IP-Adressen. Wenn wir beispielsweise ein Teilnetz 194.196.16.0 mit der Maske 255.255.255.0 besitzen, so sind die Adressen, die wir Computern im Teilnetz zuordnen können, die Adressen 194.196.16.1 bis 194.196.16.254.

Netzwerkschnittstelle

Die Netzwerkschnittstelle ist das Gerät, das den Computer über ein Kommunikationsmedium mit anderen Computern verbindet. Bei einer Netzwerkschnittstelle kann es sich um eine Ethernet-Karte, ein Modem, eine ISDN-Karte usw. handeln. Der Computer sendet und erhält Pakete über die Netzwerkschnittstelle.

P

Paket

Das Paket ist eine Standardeinheit der Datenübertragung, die angewandt wird, wenn Daten von einem Computer an einen anderen übermittelt werden. Jedes Paket enthält eine gewisse Datenmenge. Die maximale Länge eines Paketes hängt von dem jeweiligen Kommunikationsmedium ab. In Ethernet-Netzwerken beträgt die maximale Länge beispielsweise 1500 Byte. Auf jeder Ebene können wir die Inhalte der Pakete in zwei Bereiche einteilen: Den Header-Bereich und den Datenbereich. Der Header beinhaltet Kontrolldaten der speziellen Ebene, der Datenbereich beinhaltet Daten, die zur oberen Ebene gehören. Weitere Informationen über die Struktur der Pakete finden Sie im Kapitel über die Paketfilterung.

POP3

POP3-Protokoll wird meistens von E-Mail-Client-Software verwendet, um die E-Mail von den Postfächern der mit POP3 kompatiblen Mail-Servern abzuholen. Auch der Mail-Server von WinRoute verfügt über eine solche Funktion. Das bedeutet, er kann die E-Mail automatisch bei jedem mit POP3 kompatiblen Mail-Server abholen und diese weiter an die Postfächer lokaler Empfänger verteilen.

POP3-Protokoll ist ein **TCP-**Protokoll, das an **Anschluss 110** ausgeführt wird. Wenn Sie auf diesen Protokoll-Mail-Server zugreifen möchten, der hinter oder auf dem WinRoute-Computer ausgeführt wird, (um Ihre E-Mail AUS dem Internet abzuholen), müssen Sie die **Anschlusszuordnung** für das TCP- Protokoll durchführen. Anschluss 110 sendet die E-Mails an die **private** IP-Adresse des PCs, der den Mail-Server ausführt.

Postfächer in WinRoute

Die Postfächer werden in einem separaten Verzeichnis angeordnet, in dem WinRoute installiert wurde. In der Regel ist dieses Verzeichnis c:/Programm-Dateien/WinRoute/Mail.

Nach der Installation werden keine Postfächer eingerichtet, auch nicht, wenn Benutzer eingerichtet werden. Die Postfächer werden in der Regel erst eingerichtet, NACHDEM die erste E-Mail für einen Benutzer eingegangen ist.

PPTP

PPTP - Point To Point Tunnelling Protocol - ist ein VPN-Protokoll, das vom Microsoft-Betriebssystem verwendet wird, um eine verschlüsselte Verbindung zwischen zwei Computern herzustellen.

Protokoll

Legt die Richtlinien für die Datenübertragung fest.

Proxy

Proxy ist eine weitere Art des gemeinsam genutzten Internetzugangs. Proxy bearbeitet die Daten auf einer höheren Protokollebene, wodurch der gemeinsame Interentzugriff nicht zuverlässig funktionierte und für jedes Netzwerkprotokoll ein spezieller Gateway für Anwendungen erforderlich war.

R

RAS

Remote Access Service bezieht sich auf die Ferneinwahl in einen anderen Computer bzw. den Zugriff auf ein externes Netzwerk. Im Zusammenhang mit WinRoute handelt es sich bei RAS lediglich um eine DFÜ-Verbindung.

Routing-Tabelle

Routing-Tabellen fassen die vom Microsoft-Betriebssystem generierten Kriterien zusammen. Diese basieren auf den Einstellungen, die Sie in den Protokolleinstellungen für TCP/IP festlegen. Die Routing-Tabelle wird von WinRoute für die Umleitung von Paketen genutzt. Um sich die Routing-Tabelle anzeigen zu lassen, geben Sie in der MS-DOS-Eingabeaufforderung den Befehl `"route print"` ein.

S

SMTP

SMTP (Simple Mail Transfer Protocol) wird für die direkte Kommunikation zwischen den Mail-Servern (wie dem Mail-Server in WinRoute und den Mail-Server Ihres Diensteanbieters) verwendet sowie für den E-Mail-Versand über Ihre E-Mail-Client-Software. SMTP ist ein "Einweg"-Protokoll - d. h. der Mail-Server kann E-Mails versenden oder empfangen. Es ist jedoch nicht möglich, E-Mails bei einem anderen Mail-Server, der dieses Protokoll verwendet, abzuholen.

SMTP-Protokoll ist ein TCP-Protokoll, das an **Anschluss 25** ausgeführt wird. Wenn Sie auf dieses Protokoll mit dem Mail-Server, der hinter oder am WinRoute-Computer ausgeführt wird, zugreifen möchten (um anderen Mail-Servern das Recht einzuräumen, Ihnen E-Mails zu senden oder um diesen Mail-Server für den Versand Ihrer E-Mails einzusetzen, wenn Sie sich in Ihrem LAN befinden), müssen Sie die **Anschlusszuordnung** für das TCP-Protokoll durchführen. Anschluss 25 sendet die E-Mails an die **private** IP-Adresse des PCs, auf dem der Mail-Server ausgeführt wird.

T

TCP/IP

TCP/IP ist eine Zusammenfassung von Netzwerkprotokollen, die für die Kommunikation zwischen mehreren Computern verwendet wird. Alle Protokolle basieren auf Paketen. Das bedeutet, dass alle versandten Daten in kleine Bereiche aufgeteilt und über das Netzwerk versandt werden. Zu den TCP/IP-Protokollen gehören: IP, TCP, UDP, ICMP und andere auf IP-Adressen basierende Protokolle.

U

UDP

User Datagram Protocol verwendet einen speziellen Pakettyp, der Datagramm genannt wird. Datagramme erfordern keine Antwort und werden nur in eine Richtung ausgeführt. Datagramme werden vor allem für Streaming-Media verwendet, da ein gelegentlicher Paketverlust das endgültige Produkt der Übertragung nicht negativ beeinflusst.



V

VPN

Virtual Private Network betrifft lokale Netzwerke mit der Fähigkeit, Ressourcen über das Internet gemeinsam zu nutzen, indem ein direkter Tunnel erstellt wird, der an beiden Enden eine Ver-und Entschlüsselung ausführt. WinRoute unterstützt VPN über PPTP.

INDEX

A

B

C

D

K

L

M

N

P

Q